VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Srovnání parametrů a funkcí směrovačů Huawei a Cisco

Comparison of Parameters and Functions of Huawei and Cisco Routers

2013 **Michal Tabaček**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Michal Tabaček**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R059 Mobilní technologie

Téma: Srovnání parametrů a funkcí směrovačů Huawei a Cisco
Comparison of Parameters and Functions of Huawei and Cisco Routers

Zásady pro vypracování:

Cílem bakalářské práce je srovnat parametry a funkce směrovačů dvou různých výrobců - Cisco a Huawei.

Osnova práce:
1. Popište základní parametry a funkce směrovačů Huawei a Cisco.
2. V laboratorním prostředí otestujte alespoň 3 funkce obou typů zařízení.
3. Ověřte kompatibilitu obou typů zařízení.

Seznam doporučené odborné literatury:

Dokumentace k zařízením Huawei a Cisco.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Petr Machník, Ph.D.**

Datum zadání: 16.11.2012

Datum odevzdání: 07.05.2013

prof. RNDr. Vladimír Vašinek, CSc.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

Dne: *2.5 2013*

……..……

podpis studenta

Poděkování

Rád bych poděkoval panu Ing. Petru Machníkovi, Ph.D. za odbornou pomoc a konzultaci při vytváření této bakalářské práce.

Abstrakt

Tato bakalářská práce se zabývá srovnáním parametrů a funkcí směrovačů od společnosti Huawei a Cisco. Úvodní část se věnuje teoretickému popisu směrovačů od výrobce Huawei a srovnání jeho jednotlivých řad. Po seznámení se směrovači od společnosti Huawei následuje popis zařízení od společnosti Cisco a jeho porovnání s Huawei. V další části je popsáno testování funkcí na dostupných zařízeních, které probíhalo v laboratorním prostředí. Tato druhá část obsahuje základní seznámení s testovanou funkcí, postup konfigurace se zaměřením na směrovače od společnosti Huawei. Nakonec je u každé testované funkce mezi směrovači ověřena funkčnost a kompatibilita.

Klíčová slova

Směrovač, síť, Huawei, Cisco, směrovací protokol, OSPF, IPSec, MPLS, IPv6, konfigurace, funkce, parametr, kompatibilita.

Abstract

This bachelor thesis is comparing parameters and functions of Huawei and Cisco routers. Opening section is dedicated to the theoretical description of Huawei routers and to comparison of their device series. Introduction of Huawei routers is followed by description of Cisco devices and their comparison to Huawei. Functions testing of available devices, which took place in laboratory environment, is described in next section. This second section include basic introduction of each tested function and the procedure of configuration focusing on Huawei routers. Functionality and compatibility of every tested function between routers is verified in the end.

Key words

Router, network, Huawei, Cisco, routing protocol, OSPF, IPSec, MPLS, IPv6, configuration, function, parameter, compatibility.

Seznam použitých zkratek

Zkratka	Anglický význam	Český význam
3G	Third generation of mobile telecommunications technology	Zkratka pro sítě 3. generace mobilních telefonů
ADSL	Asymetric Digital Subscriber Line	Asymetrická digitální účastnická linka
AES	Advanced Encryption Standard	Pokročilý šifrovací standard
AS	Autonomous System	Autonomní systém
BDR	Backup Designated Router	Záložní pověřený směrovač
BGP	Border Gateway Protocol	Směrovací protokol BGP
DES	Data Encryption Standard	Standard šifrování dat
DR	Designated Router	Aktivní pověřený směrovač
DSP	Digital Signal Processor	Digitální signálový procesor
EIGRP	Enhanced Interior Gateway Routing Protocol	Proprietální protokol Cisco
EPON	Ethernet Passive Optical Network	Pasivní optická síť EPON
FXO	Foreign Exchange Office	Připojení do klasické analogové telefonní sítě
FXS	Foreign Exchange Station	Připojení analogového telefonu
GPON	Gigabit Passive Optical Network	Pasivní optická síť GPON
GRE	Generic Routing Encapsulation	Generické zapouzdření cesty
ICMP	Internet Control Message Protocol	Protokol řídících zpráv Internetu
IKE	Internet Key Exchange	Protokol pro vyjednání SA
IOS	Internetwork Operating System	Operační systém Cisco zařízení
IPSec	Internet Protocol Security	Bezpečnostní rozšíření IP protokolu
ISDN	Integrated Services Digital Network	Digitální komunikační síť s integrovanými službami
IS-IS	Intermediate System to Intermediate System Protocol	Dynamický směrovací protokol
ISP	Internet Service Provider	Poskytovatel služeb Internetu
IVR	Interactive Voice Response	Interaktivní hlasová odezva
LTE	Long Term Evolution	Technologie určená pro vysokorychlostní Internet v mobilních sítích

MAC Adresa	Media Access Control Address	Jedinečný identifikátor síťového zařízení
MD5	Message Digest 5	Šifrovací hash funkce
OS	Operating system	Operační systém
OSPF	Open Shortest Path First	Interní směrovací protokol
PBX	Private branch exchange	Pobočková telefonní ústředna
PoE	Power over Ethernet	Napájení po síťovém kabelu
PSK	Pre-Shared Key	Sdílený tajný klíč
PSTN	Public Switched Telephone Network	Veřejná komutační telefonní síť
RADIUS	Remote Authentication Dial In User Service	Uživatelská vytáčená služba pro vzdálenou autentizaci
RIP	Routing Information Protocol	Interní směrovací protokol
SA	Security Association	Bezpečnostní asociace
SHA	Secure Hashing Algorithm	Bezpečnostní hash algoritmus
SHDSL	Single pair High speed Digital Subscriber Line	Symetrická digitální účastnická přípojka
SIP	Session Initiation Protocol	Protokol pro inicializaci relací
SOHO	Small Office - Home Office	Malá domácí kancelář
SRU	The Switch and Route Processing Unit	Hlavní ovládací deska zařízení
SSH	Secure Shell	Zabezpečený komunikační protokol
TTL	Time to live	Parametr životnosti paketů
USB	Universal Serial Bus	Univerzální sériová sběrnice
VDSL	Very High Bit Rate Digital Subcriber Line	Vysokorychlostní DSL
VoIP	Voice over Internet Protocol	Internetová telefonie
VPN	Virtual Private Network	Virtuální soukromá síť
VRP	Versatile Routing Platform	Operační systém Huawei zařízení
WAN	Wide Area Network	Rozlehlá počítačová síť
WLAN	Wireless Local Area Network	Bezdrátová komunikace v počítačových sítích
xDSL	Digital Subscriber Line	Technologie pro přenos dat

Obsah

1 Úvod

V dnešním světě počítačových sítí a internetu si můžeme jen těžko představit, že by zařízení jako směrovače neexistovala. Internet jsou volně propojené počítačové sítě, které spojují jednotlivé síťové uzly. Uzlem může být nejen počítač, ale i specializované zařízení (směrovač). Směrovač je v počítačových sítích aktivní síťové zařízení, které procesem směrování přeposílá datagramy směrem k jejich cíli. Směrování probíhá na třetí síťové vrstvě referenčního modelu ISO/OSI.

Bakalářská práce, jak již název napovídá, pojednává o testování a srovnání směrovačů dvou výrobců – Huawei a Cisco. Pravidelně navštěvuji kurzy Cisco Academy VŠB-TUO. Zde jsem se seznámil se zařízeními od společnosti Cisco a v průběhu jsem dostal zájem poznat zařízení od jiných výrobců. Katedra telekomunikační techniky VŠB-TUO má zapůjčena zařízení od společnosti Huawei, což mě zaujalo, a proto jsem si zvolil tohle téma k mé bakalářské práci. Průběh práce je více zaměřen na tyto zapůjčené směrovače od společnosti Huawei.

V první části popíši základní vlastnosti a rozdělení jednotlivých řad směrovačů od výrobce Huawei. Uvedu zde obecné parametry, funkce a služby těchto zařízení. Po seznámení se směrovači Huawei je další kapitola věnována popisu směrovače od společnosti Cisco. V závěru této teoretické části srovnávám směrovač od výrobce Cisco se směrovačem Huawei.

Nejdůležitější částí této bakalářské práce je následné testování funkcí na směrovačích. Jako první funkce bude testován směrovací protokol OSPF, následně zabezpečená komunikace IPSec. Další dvě funkce pro testování jsou technologie MPLS a ověření podpory IPv6. Testování bude probíhat v laboratorním prostředí, a to tím způsobem, že ke každé testované funkci navrhnu zapojení sítě. Síť bude obsahovat směrovače od obou výrobců a zároveň bude ihned ověřována kompatibilita mezi zařízeními. Výstupem této části bude poté základní popis testované funkce a jak postupovat při konfiguraci na směrovačích Huawei. Pomocí softwaru Wireshark odchytím komunikaci v zapojené síti. Nakonec u každé funkce popíši ověření funkčnosti a kompatibility na získaných výstupech ze směrovačů a odchycené komunikaci ze softwaru Wireshark.

2 Vlastnosti a srovnání řad Huawei AR

2.1 Úvod k řadám a zařízením

V následující kapitole jsou popsány a srovnány řady směrovačů firmy Huawei, jedná se o řady AR1200, AR2200, AR3200. U zmíněných řad bude rozebráno, jaké nabízí modely, jejich základní parametry, rozdíly mezi řadami a oblast použití.

Směrovače Huawei AR jsou generace síťových produktů pro podniky a jejich pobočky, které nabízejí různé vlastnosti a funkce. Jsou založeny na univerzální platformě Huawei VRP (Versatile routing platform), jedná se o síťový operační systém těchto zařízení. Směrovače v sobě integrují několik funkcí: směrování, všechny již dnes standardizované směrovací protokoly pro IPv4 a IPv6, další funkce jsou 3G, WLAN, hlasové a bezpečnostní funkce. Tyto směrovače využívají vícejádrové procesory.

Směrovače podporují různé rozšiřující karty, zahrnující L2/L3 Ethernet karty, ISDN, EPON/GPON a 3G karty, synchronní/asynchronní karty. Dále ADSL2+/G.SHDSL/VDSL2 karty, FXS/FXO pro hlasové funkce. V závislosti na typu slotu jsou tyto karty rozděleny na SIC (Smart Interface Card), WSIC (Double-Width SIC) s dvojitou šířkou SIC karty a XSIC (Double-Height WSIC) s dvojitou výškou WSIC karty. Směrovače vždy tedy nabízí určité množství zmíněných slotů, tyto sloty je možné také kombinovat mezi sebou. To znamená, že například místo dvou SIC karet můžeme do směrovače vložit jednu WSIC kartu. Více informací, znázornění slotů a jejich kombinace na jednotlivých směrovačích je zobrazeno v příloze A. [1]

2.2 Vlastnosti a parametry těchto zařízení

2.2.1 Přehled vlastností a služeb

- Vkládání a vyjímání rozšiřitelných karet za chodu.
- OSP (Open Service Platform) – služba poskytuje připojení třetích stran k zařízení.
- Kompletní bezpečnostní mechanismy.
- USB auto-config funkce.
- Připojení k internetu přes rozhraní: Ethernet, xDSL, 3G, WLAN.
- Podpora hlasových funkcí – FXS/FXO porty, ISDN, PBX funkce.
- Podpora L2/L3 karet - až 24 portů na jedné kartě s rychlostí 1Gbit/s.
- ADSL 2+ Annex B karta.
- Statické směrování.
- Směrovací protokoly RIP, OSPF, IS-IS, BGP.
- IPSec VPN a GRE VPN.
- Služby pro správu NetStream, QinQ. [3]

2.2.2 Integrované služby podrobněji

Open Service Platform – směrovače AR nabízejí připojení třetích stran pomocí služby Open Service Platform. OSP tak poskytuje jednotné komunikační řešení pro podnikové uživatele. Dovoluje se připojit třetím stranám. Poskytuje rychlý servis a zjednodušení správy.

Hlasové služby – směrovače poskytují různé hlasové služby pro datové sítě. Nabízí základní hlasové funkce poskytované vestavěným PBX. Dále SIP server, IVR automatické připojení, paralelní a sekvenční vyzvánění. Inteligentní směrování hovorů a detekci kvality hlasových služeb v reálném čase. Propojení s PBX terminály běžných prodejců.

Zabezpečení – směrovače poskytují kompletní bezpečnostní ochranný mechanizmus, zahrnující řízení přístupu uživatelů, detekci pomocí paketů. Dále je obsažen vestavěný firewall, VPN technologie, IPSec a GRE metody ověřování, včetně RADIUS. Ověřovací technologie na portech, autentizace pomocí MAC adres.

Inteligentní služba – AR řada poskytuje mini-USB port. Pomocí mini-USB portu mohou uživatelé konfigurovat zařízení přes grafické uživatelské rozhraní. Směrovače podporují funkci auto-config, která umožňuje automaticky získat nastavení.

Zjednodušená správa služeb – uživatelé vyžadují jednoduché řízení služeb, tyto směrovače poskytují pro zjednodušení správy několik funkcí. Je zde funkce NQA (Network Quality Analyzer) pro sledování linek v reálném čase. Pomocí NetStream služby mohou uživatelé vidět provozní charakteristiky a statistiky a na jejich základě poté jasně určit co je potřeba udělat pro optimalizaci sítě. [2]

2.3 Základní rozdělení řad

Základní rozdělení jednotlivých řad je dle použité oblasti a možného počtu připojených uživatelů. U vyššího modelu AR2240 z řady AR2200 je udávané množství uživatelů až 250. Níže lze vidět rozdělení jednotlivých řad dle oblasti a doporučeného počtu uživatelů.

Řada AR3200

- Headquarter (sídlo, centrála) - 150 až 500 uživatelů.

Řada AR2200

- Medium branch (střední pobočky) - 50 až 150 uživatelů.

Řada AR1200

- Small branch (malé pobočky) - 10 až 50 uživatelů.

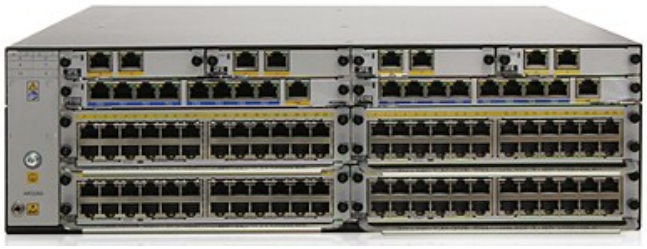
Lze ještě dodatkově přidat řadu AR200

- SOHO - Small Office Home Office (kanceláře) - 3 až 10 uživatelů. [7]

2.4 Srovnání jednotlivých řad

2.4.1 Řada AR3200

Huawei AR3200 je nejvyšší řada těchto směrovačů, která nabízí právě jeden model AR3260. Tento směrovač je určen pro využití v tzv. Headquarters (sídlech), je stavěn přibližně pro 150 až 500 uživatelů. Využíván je například tam, kde je požadavek na vysoký datový tok a přístup velkého množství uživatelů. AR3260 se oproti nižším řadám liší hlavně svým výkonem a větším počtem rozšiřovacích slotů (4*SIC + 2*WSIC + 4*XSIC). Celkově tento směrovač obsahuje pro rozšíření 10 slotů. Další odlišné parametry jsou přenosové rychlosti, které jsou zde kvůli oblastí použití vyšší než u ostatních řad. Oproti řadě AR1200 má AR3260 větší paměť RAM, podporu MicroSD karet, další vlastností je možnost výměny až dvou SRU (The Switch and Route Processing Unit) jednotek, což je v podstatě základní ovládací deska zařízení, více o SRU jednotce v příloze A. Od řad AR1200 a AR2200 se také liší procesorem. S podporou více slotů a větším výkonem je rovněž spojena samozřejmě větší spotřeba elektrické energie. Maximální spotřeba je zde 179W, tato spotřeba je v případě, když směrovač neobsahuje žádné rozšiřovací karty. V případě osazení rozšiřovacími kartami je spotřeba větší. Směrovač podporuje zpracování telefonních hovorů. Na obrázku 2.1 lze vidět jediný model z této řady.



Obrázek 2.1: Směrovač AR3260 [4]

Směrovač AR3260 nabízí bezdrátový přístupový režim a přístupový režim přes kabeláž. Bezdrátový režim nabízí 3G a LTE přístupové metody. Podporuje přechod z 3G sítě na budoucí LTE sítě, které se začínají rozšiřovat. Přístup přes kabeláž využívá optické a metalické kabely. Podporuje Gigabit Ethernet, CPOS optické rozhraní, xDSL rozhraní, sériové porty, ISDN rozhraní, ale nepodporuje WLAN přístup jako řada AR1200.

2.4.2 Řada AR2200

Huawei AR2200 je střední řada, ta nabízí dva směrovače AR2220 a AR2240. Tyto směrovače jsou určeny pro využití v tzv. Medium branch (středních pobočkách), jsou stavěny přibližně pro 50 až 150 uživatelů. Co se týče funkcí nabízených v této řadě, od řady AR3200 se neliší. Integrované služby a funkce jsou stejné jako u AR3260. Taktéž paměť RAM a paměť Flash jsou stejné. Jedním z hlavních rozdílů je možnost rozšiřitelnosti, řada AR2200 nabízí méně slotů. Model AR2220 obsahuje 6 slotů (4*SIC + 2*WSIC) a model AR2240 obsahuje celkově 8 slotů (4*SIC + 2*WSIC + 2*XSIC). S menším počtem slotů je spojena i menší spotřeba elektrické energie. Dalším rozdílným parametrem jsou menší přenosové rychlosti a procesor s méně jádry, model AR2220 je vybaven 4-jádrovým procesor a model AR2240 obsahuje 8-jádrový procesor. Směrovač AR3260 může obsahovat až 12- jádrový procesor, záleží na tom, jaká SRU jednotka je ve směrovači. SRU jednotky lze měnit pouze v modelech AR2240 a AR3260, více informací o SRU v příloze A. Na obrázku 2.2 a 2.3 lze vidět směrovače z této řady.

Obrázek 2.2: Směrovač AR2220 [5]

Obrázek 2.3: Směrovač AR2240 [5]

2.4.3 **Řada AR1200**

Huawei AR1200 je nejnižší řada z uvedených, nabízí celkem 4 směrovače AR1220, AR1220V, AR1220W a AR1220VW. Tyto směrovače jsou určeny pro tzv. Small branch (malé pobočky), jsou stavěny přibližně pro 10 až 50 uživatelů. Co se týče nabízených funkcí a softwaru v této řadě, od řady AR3200 a AR2200 není moc odlišná. Mění se hlavně hardwarové parametry. Paměť RAM je zde 512 MB, řada AR2200 a AR3200 má paměť RAM 2GB. Paměť Flash je zde 256 MB, u AR2200 a AR3200 je to pouze 16 MB. U řady AR1200 ovšem chybí podpora MicroSD, díky které u vyšších řad můžeme rozšířit paměť Flash až na 4 GB.

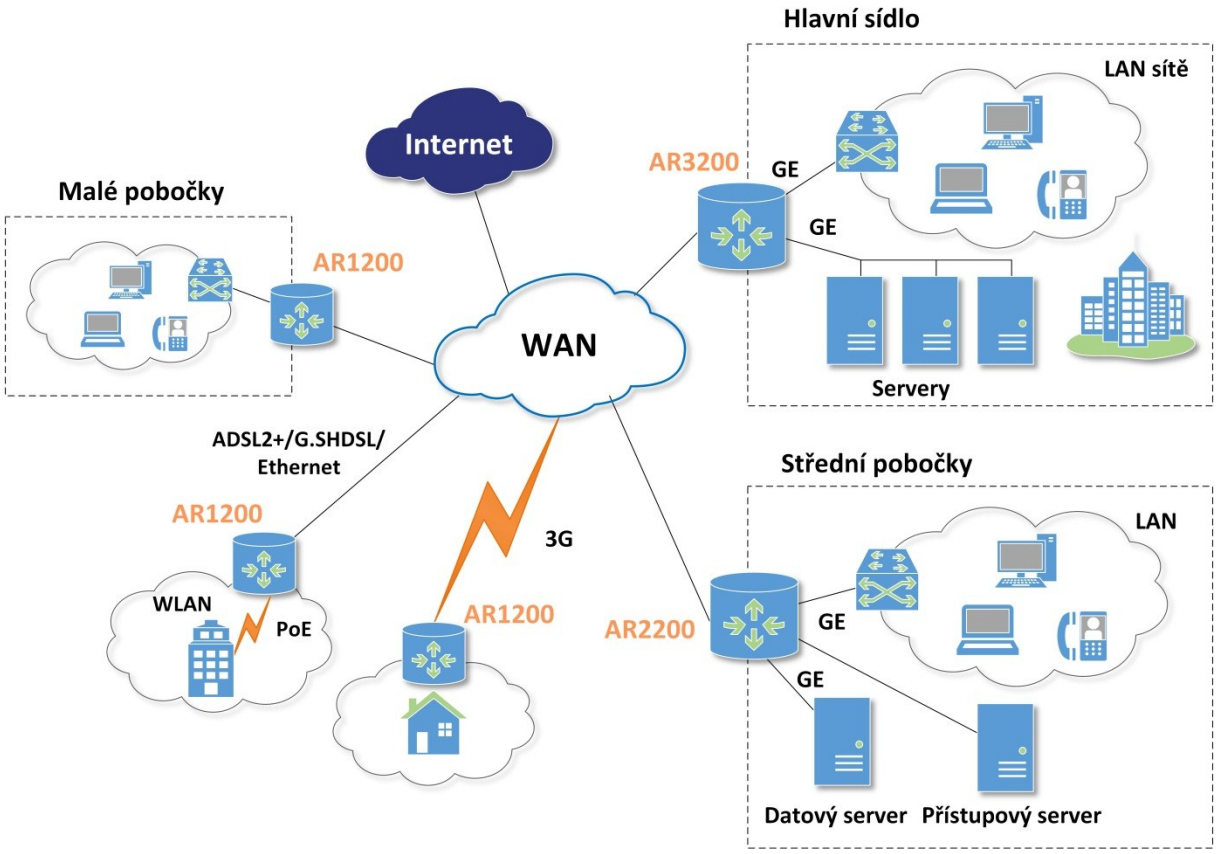
Dalšími rozdíly je rozšiřitelnost, řada AR1200 má pouze 2 sloty (2*SIC) a nejmenší spotřebu elektrické energie. Poskytuje menší přenosové rychlosti oproti řadám AR2200 a AR3200. Je zde k dispozici podpora Gigabit Ethernet, xDSL rozhraní, sériové porty, ISDN rozhraní, navíc také podpora WLAN přístupu. Modely AR1220V, AR1220W a AR1220VW oproti řadám AR2200 a AR3200 poskytují funkci PoE (Power over Ethernet), což je napájení po datovém síťovém kabelu bez nutnosti přivést napájecí napětí k přístroji dalším samostatným kabelem. Směrovače podporují funkci PoE na svých čtyřech Fast Ethernet portech.

Obrázek 2.4: Směrovače AR1200 [6]

Na obrázku 2.4 můžeme vidět směrovače řady AR1200. Na levé straně se jedná o model AR1220 a AR1220V, které jsou na pohled stejné, liší se hlavně v podpoře PoE. Po pravé straně se nachází model AR1220VW a AR1220W. Tyto směrovače se oproti AR1220 a AR1220V, jak lze vidět z obrázku, liší v podpoře WLAN přístupu.

2.5 Typické použití

Řada AR3200, jak již bylo řečeno, je využívána tam, kde je požadavek na vysoký datový tok a přístup velkého množství uživatelů. Jedno z typických použití tohoto směrovače je v připojení celého sídla (Headquarters) do WAN sítě. Další využití je například v oblasti hlasových služeb pro podnikové sítě, kde řada AR3200 může fungovat například jako IP PBX u hlavních sídel. AR3200 také poskytuje zabezpečené přístupové funkce VPN, díky kterým lze provádět zabezpečenou komunikaci. Řada AR2200 může být použita v případech, které jsou popsány u řady AR3200. Rozdíl je zde v tom, že řada AR2200 se použije většinou u středních poboček a externích pracovníků. Dále také lze u řady AR2200 použít 3G datový bezdrátový přístup. U řady AR1200 je jedno z typických použití přístup do WAN sítě, kde jsou ve funkci jako výstupní směrovače malých poboček. K připojení do sítě je zde například použito rozhraní pevné linky, rozhraní Ethernet, xDSL a 3G. Navíc je zde podpora WLAN připojení k tomuto směrovači u dvou nabízených modelů. Dále například již řečené hlasové služby, zabezpečená komunikace VPN.



Obrázek 2.5: Schéma použití směrovačů

Na obrázku 2.5 je zobrazeno schéma jednoho z typických použití směrovačů řad AR1200, AR2200 a AR3200. Lze vidět použití řady AR3200 pro připojení hlavního sídla do WAN sítě, v hlavním sídle je obsaženo několik LAN sítí, servery a další. Řada AR2200 připojuje střední pobočky, obsahuje také LAN sítě, zde již je ale méně uživatelů. Nejnižší řada AR1200 zobrazuje připojení menších poboček. Více informací a schémat o použití jednotlivých směrovačů, které byly zmíněny v této podkapitole, se lze dočíst v dokumentech od společnosti Huawei zde [1] [2] [3].

2.6 Srovnání a přehled parametrů v tabulce

Níže v Tabulce 2.1 jsou pro přehlednost zobrazeny základní hardwarové parametry. Jsou zde navzájem srovnány všechny modely. Parametr forwarding capacity je udáván v Kpps (tisíc paketu za sekundu) nebo Mpps (milión paketů za sekundu). Pro převod na jednotky například Mbit/s závisí na tom, kolik bitů očekáváme v paketu. Paket Ethernet se může pohybovat mezi 64 - 1500 bytů (512 - 12000 bitů). Pro forwarding capacity 350 Kpps vychází hodnota přibližně 200Mbit/s při délce paketu 64 bytů. Kompletní rozsáhlá tabulka hardwarových a softwarových parametrů se nachází v příloze B.

Tabulka 2.1: Přehled parametrů směrovačů Huawei

	AR1220	**AR1220V AR1220W AR1220VW**	**AR2220**	**AR2240**	**AR3260**
Forwarding capacity	350 Kpps	350 Kpps	1 Mpps	2 Mpps (standard)	2 Mpps (standard)
WAN speed With services	25 Mbit/s	25 Mbit/s	75 Mbit/s	150 Mbit/s	1000 Mbit/s
Switching capacity	8 Gbit/s	8Gbit/s	32 Gbit/s	80 Gbit/s	160 Gbit/s
WAN porty	2*GE	2*GE	3*GE	3*GE	3*GE
LAN porty	8*FE	8*FE	-	-	-
SIC sloty	2	2	4	4	4
WSIC sloty	-	-	2	2	2
XSIC sloty	-	-	-	2	4
PoE	-	4*FE	-	-	-
Wifi	-	802.11 b/g/n	-	-	-
USB 2.0	2	2	2	2	2
Mini-USB	1	1	1	1	1
Paměť	512 MB	512 MB	2 GB	2 GB	2 GB
Paměť Flash	256 MB	256 MB	16 MB	16 MB	16MB
MicroSD	-	-	Max. 4 GB	Max. 4 GB	Max. 4 GB

3 Srovnání směrovačů Huawei a Cisco

V následující kapitole bude popsán směrovač Cisco 2801 a porovnán se směrovačem Huawei AR2220. Tyto dva směrovače jsou přibližně ve stejné kategorii a úrovni použití. Směrovač AR2220 zde již nebude samostatně popsán, toto zařízení bylo dostatečně probráno v hlavní kapitole 2. Směrovač Cisco 2801 je také k dispozici pro laboratorní měření a pro ověřování vzájemné kompatibility se směrovači Huawei.

3.1 Cisco 2801

3.1.1 Obecný popis řady Cisco 2800 a směrovače Cisco 2801

Řada směrovačů Cisco 2800 jsou síťové produkty pro podniky a jejich pobočky. Nabízí různé integrované služby a vlastnosti. Směrovače a také přepínače Cisco jsou založeny na platformě Cisco IOS (Internetwork Operating System), což je operační systém těchto zařízení. IOS je balíček směrovacích, přepínacích, propojovacích a telekomunikačních funkcí pevně integrovaný do multitaskingového operačního systému. Směrovače Cisco v sobě obsahují různé funkce, jako jsou například směrování (směrovací protokoly pro IPv4 a IPv6), hlasové a bezpečnostní funkce. Dále nabízí možnost připojení přes xDSL rozhraní a také podporuje funkce zpracování telefonních hovorů. Řada Cisco 2800 se skládá ze čtyř modelů Cisco 2801, Cisco 2811, Cisco 2821 a Cisco 2851. [8]

Všechny modely směrovačů z řady Cisco 2800 si můžeme pomocí rozšiřitelných karet značně rozšířit a získat tak více funkcí. Počet a typ slotů pro tyto karty se liší podle použitého směrovače. V závislosti na typu slotu jsou rozšiřující karty rozděleny na karty WAN rozhraní (WIC), karty hlasového rozhraní (VIC), hlasové/WAN karty (VWIC) a vysokorychlostní WAN karty (HWIC). Sloty na směrovači podporují různé duhy karet, například směrovač 2801 obsahuje jeden slot označen jako VIC/VWIC, jiné typy karet tento slot nepodporuje.

3.1.2 Přehled vlastností a služeb

- Podpora hlasových funkcí, IP telefonie, FXS/FXO porty, ISDN.
- Možnost rozšiřitelnosti pomocí karet.
- Bezpečnostní mechanismy, URL filtr.
- IOS firewall, SSH, služba NAC.
- Připojení k internetu přes: Ethernet, xDSL, 3G, WLAN.
- Zabezpečená komunikace IPSec VPN a GRE VPN.
- ADSL, G.SHDSL a 3G rozhraní.
- Směrovací protokoly RIP, OSPF, EIGRP, BGP.
- Statické směrování.
- Podpora funkce PoE (Power over Ethernet).
- Chybí zde podpora Gigabit Ethernet. [8] [10]

Obrázek 3.1: Směrovač Cisco 2801[11]

3.1.3 Funkce a vlastnosti podrobněji

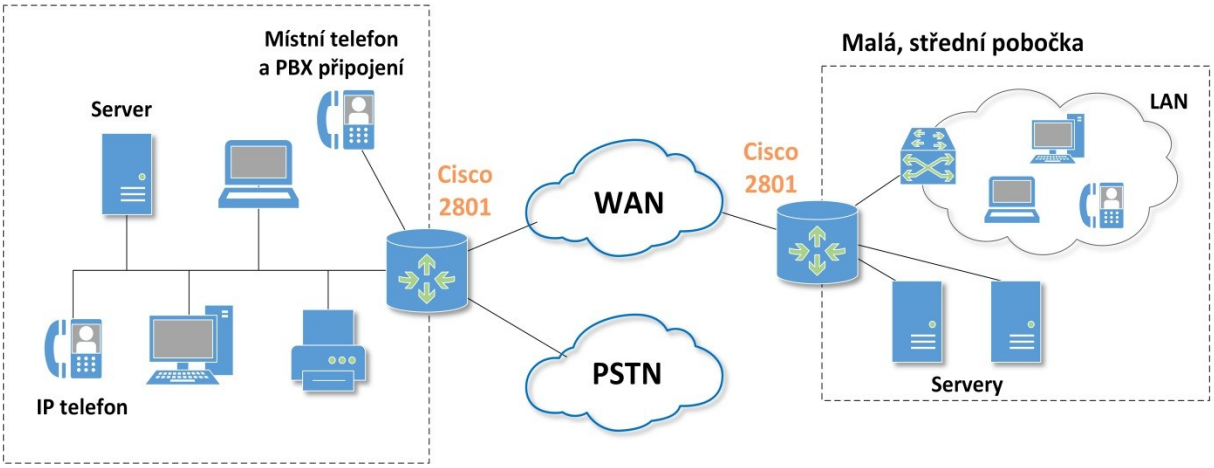
Rozšíření – směrovač Cisco 2801 obsahuje celkově 4 sloty pro rozšíření. Nabízí 2 sloty podporující HWIC/WIC/VIC/VWIC, tyto sloty jsou schopné podporovat karty HWIC s klasickou šířkou jednoho slotu, ale také s dvojitou šířkou. Dále nabízí jeden slot WIC/VIC/VWIC a jeden slot podporující VIC/VWIC. Směrovač obsahuje dva Fast Ethernet 10/100 porty. U směrovače Cisco 2801 chybí podpora Gigabit Ethernet, podporu Gigabit Ethernet nabízí pouze modely Cisco 2821 a 2851. Směrovač 2801 na rozšiřitelné kartě HWIC podporuje PoE funkci, PoE funkce může tedy poskytnout napájení pro kompatibilní zařízení.

Zabezpečení sítě – Cisco IOS nabízí pokročilé nastavení funkcí zabezpečení. Poskytuje Cisco IOS firewall, prevenci průniků, IPSec VPN, pokročilé aplikace inspekce a kontroly, Secure Shell (SSH), URL filtrování. Dále podporuje pro lepší zabezpečení službu NAC (Network Admission Control), která umožňuje kontrolu síťových přístupů. Obsahuje také IPS (Intrusion Prevention System - system pro prevenci útoku) a IOS WebVPN (SSL VPN) pro bezpečný vzdálený přístup pro mobilní uživatele bez nutnosti instalace softwaru.

Hlasové služby – Cisco 2801 umožňuje poskytovat analogovou a digitální telefonii. Tento směrovač nabízí technologii VoIP umožňující přenos digitalizovaného hlasu v těle paketů prostřednictvím počítačové sítě. Dále nabízí protokol pro přenos hlasu v sítích Frame Relay - VoFR (Voice over Frame Relay). Funkce CCME (Cisco CallManager Express) je řešení vložené do Cisco IOS, které poskytuje volání a zpracování pro IP telefony Cisco. Toto řešení podporuje nasazení až pro 96 IP telefonů souběžně se směrováním a dalšími službami. Uživatelé mohou bezpečně nasadit datovou a hlasovou komunikaci na jediné platformě pro jejich malé a středně velké pobočky. [9]

3.1.4 Typické použití

Použití směrovače Cisco 2801 je podobné jako tomu bylo u směrovače Huawei AR2220. Cisco 2801 můžeme použít v případě připojení malé až střední firmy do sítě WAN. Můžeme využívat zabezpečenou komunikaci pomocí VPN připojení. Nabízí se zde možnost připojení k internetu přes rozhraní jako pevná linka, Ethernet, xDSL. Dále je umožněno využívání hlasových služeb například pomocí technologie VoIP, zpracování volání a spousta již zmíněných služeb v podkapitole 3.1.3. Díky rozšíření lze také využít WLAN přístup. Na obrázku 3.2 je možno vidět schéma některých použití tohoto směrovače.



Obrázek 3.2: Schéma použití směrovače Cisco 2801

Zde na obrázku 3.2 lze vidět použití směrovače Cisco 2801, jak připojuje do sítě WAN určitou pobočku. V pobočce je poté realizována síť LAN, kde jsou připojeny servery a další zařízení. Cisco 2801 je zde využit také pro IP PBX. Není zde zobrazeno použití WLAN přístupu, kterého můžeme dosáhnout při rozšíření směrovače o HWIC kartu podporující 802.11 a/b/g jako přístupový bod. [8] [9]

3.2 Srovnání Huawei AR2220 a Cisco 2801

Pro srovnání směrovačů mezi Huawei a Cisco byly vybrány modely Huawei AR2220 a Cisco 2801. Taktéž pro laboratorní měření je od firmy Cisco k dispozici právě směrovač Cisco 2801. Při prvním pohledu na tyto dva směrovače se liší v uspořádání portů a možnosti rozšiřitelnosti. Směrovač 2801 má na zadní straně pouze zásuvku na napájení a spínač, ostatní porty a sloty pro karty jsou všechny na přední straně. AR2220 od Huawei se v tomto liší tím, že celá zadní strana obsahuje sloty pro rozšiřitelné karty a na přední straně jsou porty, USB vstupy a napájení, které je lehce vyměnitelné. Cisco 2801 nabízí pro rozšíření 4 sloty, AR2220 nabízí celkem 6 slotů. Každý směrovač má své označení slotů a karet, pro Cisco to je HWIC/WIC/VIC/VWIC a pro Huawei SIC/WSIC/XSIC, více o těchto typech v kapitolách 2.1 a 3.1.

Směrovač AR2220 nabízí porty USB 2.0, mini-USB a podporu MicroSD karet. Cisco 2801 obsahuje USB 1.1 a podpora MicroSD karet chybí, nabízí ale slot pro Compact Flash karty. AR2220 navíc obsahuje větší paměť a to 2GB, Cisco nabízí v základním vybavení paměť 128 MB rozšiřitelnou až na 384 MB. U směrovače Cisco chybí podpora Gigabit Ethernet, nepodporuje tyto porty ani po rozšíření. Cisco nabízí podporu funkce PoE, u Huawei AR2220 tato podpora chybí, nabízí ji pouze řada AR1200. Rozměry, váha a provozní podmínky jsou u těchto směrovačů velmi podobné. Směrovač Huawei AR2220 nabízí novější technologie, například USB, MicroSD karty nebo podporu Gigabit Ethernet. Je to dáno tím, že Huawei je novější zařízení než Cisco 2801. Firma Cisco již ale nabízí novější směrovače řady 2900, které nabízí mnoho dalších funkcí.

V tabulce 3.1 můžeme vidět souhrnný přehled parametrů směrovačů Huawei AR2220 a Cisco 2801, jedná se o porovnání z hardwarového hlediska. Dle nabízených funkcí jsou tyto směrovače velmi podobné, ale každá firma nabízí i něco odlišného. U směrovacích protokolů nabízí například Cisco proprietální protokol EIGRP, který je k dispozici jen na zařízeních Cisco. Směrovač Huawei nabízí své služby pro uživatele jako například OSP, NQA, NetStream. Oba směrovače nabízí různá zabezpečení, funkce VPN, MPLS a další, všechny funkce a služby jsou podrobněji rozebrány v kapitole 2.4 pro Huawei a kapitole 3.1 pro směrovač Cisco. Obsáhlá tabulka parametrů pro směrovač Cisco 2801 se nachází v příloze B.

Tabulka 3.1: Srovnání parametrů Huawei AR2220 a Cisco 2801

	Huawei AR2220	**Cisco 2801**
Rozšiřitelné sloty	6	4
DSP sloty	1	2
PoE podpora	-	Ano
USB 2.0	2	-
USB 1.1	-	1
Mini-USB	1	-
Konzolový port	1	1
WAN porty	3*GE	2*FE
Podpora Gigabit Ethernet	Ano	-
Paměť (default/max)	2 GB	128 MB/ 384 MB
Paměť Flash (default/max)	16 MB	64 MB/128 MB
MicroSD	2 GB/4 GB	-
Max. výkon napájení	150 W	120 W
Napájení AC	100V - 240V	100V - 240V
Frekvence	50Hz/60Hz	47Hz/63Hz
Rozměry (š x h x v)	442mm x 420mm x 44,5mm	439mm x 419mm x 45mm
Hmotnost (bez karet)	4,95Kg	5 Kg
Směrovací protokoly IPv4	RIP, OSPF, IS-IS, BGP	RIP, EIGRP, OSPF, BGP
Směrovací protokoly IPv6	RIPng, OSPFv3, IS-ISv6, BGP4+	EIGRP, RIPng, OSPFv3, IS-IS, BGP

4 Základní konfigurace zařízení

V následující kapitole budou nejprve popsány základní příkazy pro zařízení Huawei, jedná se například o přechody mezi konfiguračními režimy, uložení konfigurace a další. V dalších kapitolách je již popsána konfigurace a ověření kompatibility určité funkce, schéma zapojení sítě při měření v laboratoři, odchyt komunikace pomocí softwaru Wireshark, zobrazení výstupních tabulek směrovačů Huawei a Cisco a jejich následné porovnání. Níže v tabulce 4.1 lze vidět verze operačních systémů testovaných směrovačů používaných v laboratoři.

Tabulka 4.1: Přehled OS a firmware testovaných směrovačů

Zařízení	**Verze OS**
Huawei AR1220	5.120 (V200R003C00SPC200)
Huawei AR2220	5.120 (V200R003C00SPC200)
Huawei AR3260	5.120 (V200R003C00SPC200)
Cisco 2801	12.4 (C2801-ADVIPSERVICESK9-M)

4.1 Základní příkazy

Pro usnadnění používání příkazů musí být všechny zařazeny do skupin. Prostředí příkazové řádky je rozděleno do několika konfiguračních režimů neboli pohledů (zobrazení). Všechny příkazy musí být provedeny v odpovídajícím režimu příkazového řádku.

Když se uživatel přihlásí k zařízení, vidí následující režim na obrazovce - jedná se o uživatelský režim, kde může zobrazit stav chodu a statistiky zařízení.

```
<Huawei>
```

Při zadání příkazu system-view v uživatelském režimu se uživatel dostane do systémového režimu, zde může nastavovat systémové parametry a dostat se na další funkce.

```
<Huawei> system-view
[Huawei]
```

Následující příkaz umožní konfiguraci parametrů určitého rozhraní. Jedná se o fyzické atributy, protokoly linkové vrstvy a IP adresy. Gigabit Ethernet je pouze příklad.

```
[Huawei] interface gigabitethernet X/Y/Z
[Huawei-GigabitEthernetX/Y/Z]
```

Parametry pro směrovací protokoly lze nakonfigurovat v režimu pro konkrétní směrovací protokol. Při zadání příkazu směrovacího protokolu v systémovém režimu se směrovací protokol aktivuje a následně zobrazí režim pro konfiguraci, níže lze vidět příklad OSPF.

```
[Huawei] ospf
[Huawei-ospf-1]
```

Zde je uvedeno několik základních konfiguračních příkazů, první příkazy zobrazují, jak lze opouštět různé konfigurační režimy. Slouží k tomu příkaz quit nebo další možnosti.

```
[Huawei-isis-1] quit                #také Ctrl+Z nebo příkaz return
[Huawei] quit
<Huawei>
```

Pro změnu jména směrovače a následné odstranění jakéhokoli příkazu slouží následující příkazy. Další příkaz nám nastaví uvítací zprávu při přihlášení uživatele. Také je dobré používat příkaz description pro popis například rozhraní. Všude můžeme použít klávesu Tab, která je určena pro dokončení požadovaného příkazu nebo jeho části. Pokud chceme vypsat nápovědu příkazů, použijeme otazník, nebo když potřebujeme nápovědu pro dokončení konkrétního příkazu.

```
[Huawei] sysname Server
[Server] undo sysname
<Huawei> system-view
[Huawei] header login information "Hello,Welcome to Huawei!"
[Huawei-GigabitEthernet0/0/0] description text popisu
[Huawei]?
```

Zde jsou některé příkazy pro uložení konfigurace do stávajícího souboru nebo nového konfiguračního souboru, vymazání nebo zvolení konfigurace při příštím spuštění směrovače, výběr softwaru při příštím spuštění, restart zařízení.

```
<Huawei> save
<Huawei> save aa.cfg
<Huawei> reset saved-configuration
<Huawei> startup saved-configuration aa.cfg
<Huawei> startup system-software sd1:/V200R002C00.cc
<Huawei> reboot
```

Pro zjištění informací o zařízení nebo zobrazení konkrétních informací slouží příkaz display používaný v uživatelském i systémovém režimu. Níže lze vidět několik těchto základních příkazů. První příkaz nám zobrazuje verzi operačního systému. Další příkazy dispaly current-configuration a display saved-configuration nám znázorňují aktuální a uloženou konfiguraci. Pomocí posledního příkazu display startup si můžeme zobrazit soubory požívané pro spuštění směrovače.

```
<Huawei> display version
<Huawei> display current-configuration
<Huawei> display saved-configuration
<Huawei> display startup
```

Jako zdroj pro základní příkazy konfigurace směrovače Huawei byla použita konfigurační příručka, kde lze nalézt také další konfigurační příkazy [12].

5 Směrovací protokol OSPF

5.1 Základní popis OSPF

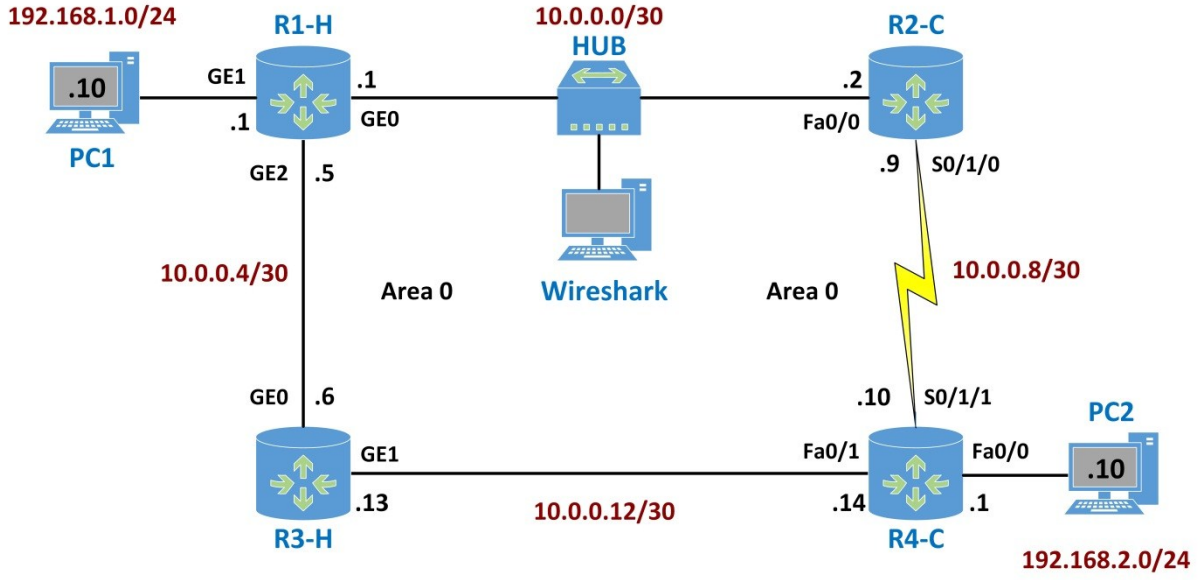
Jako první funkce pro ověření a konfiguraci bude popsán směrovací protokol OSPF (Open Shortest Path First). Ten se používá pro interní směrování uvnitř autonomního systému. OSPF je představitelem směrovacího protokolu typu Link State (na základě stavu linky). Protokol vychází z algoritmu SPF (Shortest Path First), jehož prostřednictvím každý směrovač v síti provádí výpočty potřebné k nalezení nejlepší cesty k libovolnému uzlu sítě. Směrovače si posílají hello pakety a další čtyři typy paketů, z nichž některé obsahují LSA (Link State Advertisement). Pomocí těchto zpráv provádí protokol OSPF kontrolu dostupných směrovačů a stavu připojených linek. Na základě těchto zpráv je v paměti každého směrovače v síti vytvářena a aktualizována tzv. topologická databáze. U směrovacího protokolu OSPF se nepřenáší kompletní směrovací tabulky, ale pouze změny ve stavu linek a změny sítě.

Velkou výhodou OSPF je jeho schopnost pracovat v relativně velkých sítích, u protokolu je síť rozdělená na takzvané oblasti (area), kde area 0 je považována za páteřní. LSA se běžně šíří pouze uvnitř dané oblasti a také výpočet SPF algoritmu se spouští pro každou oblast samostatně. Z jedné oblasti do druhé se předávají pouze sumární informace.

Protokol OSPF používá metriku označovanou jako cena (cost). To je číslo v rozsahu 1 až 65535, přiřazené ke každému rozhraní směrovače. Čím je číslo menší, tím má cesta lepší metriku a bude tedy více preferována. Standardně je ke každému rozhraní přiřazena cena automaticky odvozená z přenosové rychlosti daného rozhraní podle vztahu, typicky cost = 100000000 / přenosová rychlost v bit/s. [13]

5.2 Konfigurace

V následující podkapitole je popsána konfigurace směrovacího protokolu OSPF především na zařízeních Huawei. Ukázka konfigurace směrovacího protokolu OSPF na zařízení Cisco je přidána v příloze C. Na obrázku 5.1 můžeme vidět zapojení sítě, které bylo použito při testování v laboratoři.



Obrázek 5.1: Schéma zapojení sítě pro OSPF

Na obrázku 5.1 lze vidět, že byly použity čtyři směrovače, dva od firmy Huawei (R1-H a R3-H) a dva od firmy Cisco (R2-C a R4-C). Směrovače Cisco byly navzájem spojeny sériovou linkou, ostatní spoje jsou poté realizovány pomocí UTP kabelu. Směrovače Huawei nabízí porty Gigabit Ethernet, Cisco pouze Fast Ethernet. Na spojích byly umístěny dva rozbočovače se zapojenými počítači a spuštěným softwarem Wireshark pro odchyt komunikace na této lince. Dále byly zapojeny počítače PC1 a PC2, jeden ve směrovači Huawei a druhý ve směrovači Cisco, na počítačích byl nainstalován operační systém Ubuntu. Celé zapojení sítě je v jedné oblasti area 0, na tomto zapojení následovala konfigurace směrovacího protokolu OSPF a ověření funkčnosti.

Konfigurace rozhraní – zde můžeme vidět konfiguraci rozhraní na směrovači R1-H. V systémovém režimu zadáme příkaz interface a naše požadované rozhraní. Poté již stačí pomocí příkazu ip address nastavit ip adresu. Ostatní rozhraní na směrovačích Huawei se nastaví stejným způsobem.

```
<R1-H> system-view
[R1-H] interface Gigabitethernet 0/0/0
[R1-H-GigabitEthernet0/0/0] ip address 10.0.0.1 30
[R1-H-GigabitEthernet0/0/0] quit
```

Konfigurace OSPF – níže lze vidět konfiguraci směrovacího protokolu OSPF na směrovači R1-H. První nakonfigurujeme id směrovače, na ostatních směrovačích je nakonfigurováno id podle jejich čísla (například R2 - 2.2.2.2). Následně spustíme protokol OSPF a v režimu směrovacího protokolu zadáme příkaz area 0 (naše požadovaná oblast). Poté přidáme pomocí příkazu network, sítě které jsou přímo připojeny na směrovač. Tímto způsobem provedeme konfiguraci na zbývajících směrovačích.

```
[R1-H] router id 1.1.1.1
[R1-H] ospf
[R1-H-ospf-1] area 0
[R1-H-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[R1-H-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.3
[R1-H-ospf-1-area-0.0.0.0] network 10.0.0.4 0.0.0.3
[R1-H-ospf-1-area-0.0.0.0] quit
```

Konfigurace hello, dead, cost – výchozí konfigurace hello paketu je 10 sekund, dead interval je 40 sekund, časové intervaly se zadávají v sekundách. Pokud chceme upřednostnit některou linku a nechceme ceny přírazné dle stavu linky, lze si nastavit ceny linek manuálně. Veškerá tato konfigurace se provádí na určitém rozhraní požadovaného směrovače.

```
[R1-H] interface Gigabitethernet 0/0/0
[R1-H-GigabitEthernet0/0/0] ospf timer hello 10
[R1-H-GigabitEthernet0/0/0] ospf timer dead 40
[R1-H-GigabitEthernet0/0/0] quit
```

Konfigurace stub oblasti, silent rozhraní – v případě že chceme v OSPF protokolu nastavit některou oblast jako stub, stačí zadat příkaz stub v požadované oblasti. Aby určitý interface nepřijímal a neposílal updaty, použijeme příkaz silent-interface. Níže lze vidět příklad konfigurace.

```
[R1-H-ospf-1-area-0.0.0.0] stub
[R1-H-ospf-1-area-0.0.0.0] silent-interface Gigabitethernet 0/0/0
```

Příkazy pro kontrolu – zde je uvedeno několik příkazů pro kontrolu konfigurace a zobrazení informací jako například směrovací tabulka, zobrazení sousedů, rozhraní a další.

```
[R1-H]display ospf routing
[R1-H]display ospf peer
[R1-H]display ospf lsdb
[R1-H]display ospf interface
```

Konfigurace směrovače Cisco je přiložena v příloze C. Jako zdroj pro konfiguraci směrovačů Huawei byla použita konfigurační příručka [14], kde lze nalézt také další konfigurační příkazy.

5.3 Ověření funkčnosti

V této podkapitole bude popsán průběh komunikace směrovacího protokolu OSPF ze softwaru Wireshark a dále popsáno ověření funkčnosti a kompatibility. Nakonec budou porovnány výstupní směrovací tabulky ze směrovačů Huawei a Cisco.

Na obrázku 4.2 lze vidět úsek komunikace ze softwaru Wireshark, jedná se o komunikaci mezi směrovači R1 a R2, počítač s Wireshark je zapojen do HUB1. V sítí byla rozpojena a zapojena linka, poté následně sledována komunikace. OSPF komunikace využívá multicast paketů. Používají se dvě multicastové adresy 224.0.0.5 – pakety přijímají všechny směrovače, 224.0.0.6 – tyto pakety přijímá pouze DR a BDR.

Source	Destination	Protocol	Length	Info
10.0.0.2	224.0.0.5	OSPF	94	Hello Packet
10.0.0.1	224.0.0.5	OSPF	82	Hello Packet
10.0.0.1	224.0.0.5	OSPF	134	LS Update
10.0.0.1	224.0.0.5	OSPF	82	Hello Packet
10.0.0.2	224.0.0.5	OSPF	78	LS Acknowledge
10.0.0.2	224.0.0.5	OSPF	110	LS Update
10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
10.0.0.2	224.0.0.5	OSPF	94	Hello Packet
10.0.0.1	10.0.0.2	OSPF	66	DB Description
10.0.0.2	10.0.0.1	OSPF	78	DB Description
10.0.0.1	224.0.0.5	OSPF	82	Hello Packet
10.0.0.2	224.0.0.5	OSPF	94	Hello Packet

Obrázek 5.2: Ukázka komunikace OSPF ze softwaru Wireshark

Můžeme vidět, zasílání Hello paketů na multicastové 224.0.0.5, které vytvářejí a udržují vztah sousednosti mezi propojenými směrovači. Další typ paketu, který lze vidět, je Database Description tento paket se uplatní při vytváření vztahu přilehlosti mezi směrovači, je určen pro budování databáze topologie sítě. Paket Link State Update se používá pro šíření LSA po síti, zasílá se při změně parametrů linky. Paket Link State Acknowledgement potvrzuje platnost změny parametrů přijatých v paketech Link State Update. Více LSA může být potvrzeno v jednom Link State Acknowledgement paketu. Poslední typ paketu, který na obrázku 4.2 není vidět, je paket Link State Request. Tento paket pošle směrovač svému sousedovi v případě, když zjistí, že mu některé LSA chybí. Odpovědí na tento Link State Request je paket LS Update. Na obrázku je vidět klasické zasílání Hello paketů, následuje paket LS Update, který zasílá směrovač R1, od směrovače R2 přichází LS Acknowledge. Dále oba směrovače zaslali zprávu Database Description.

V následující ukázce můžeme vidět směrovací tabulku protokolu OSPF ze směrovače R3 od firmy Huawei. Po zadání příkazu lze vidět přehledně jednotlivé sítě, celkové ceny k této síti. Dále se jedná o dva typy oblastí – Transit nebo Stub. Tranzitní oblast je taková, kterou prochází provoz z jedné oblasti do druhé. Ve stub oblasti všechen provoz začíná nebo končí, ale nikdy jí neprochází. Dále můžeme vidět, v jaké oblasti sítě jsou, a také takzvaný NextHop neboli rozhraní směrovače, přes který se dostaneme do určité sítě.

```
[R3-H]display ospf 1 routing

          OSPF Process 1 with Router ID 3.3.3.3

                    Routing Tables

Routing for Network

Destination     Cost  Type      NextHop     AdvRouter    Area

10.0.0.4/30     1     Transit   10.0.0.6    3.3.3.3      0.0.0.0

10.0.0.12/30    1     Transit   10.0.0.13   3.3.3.3      0.0.0.0

10.0.0.0/30     11    Transit   10.0.0.5    1.1.1.1      0.0.0.0

10.0.0.8/30     782   Transit   10.0.0.14   4.4.4.4      0.0.0.0

192.168.1.0/24  2     Stub      10.0.0.5    1.1.1.1      0.0.0.0

192.168.2.0/24  2     Stub      10.0.0.14   4.4.4.4      0.0.0.0

Total Nets: 6

Intra Area: 6  Inter Area: 0  ASE: 0  NSSA: 0
```

Všechny sítě až na dvě dostaly cenu 1, linka mezi R2- a R4-C propojená sériovou linkou má cenu 781, což odpovídá předpokladům (cena = 100000000/128000 = 781). Pro rychlosti od 100Mbit/s a výše je cena linky stejná a určena cenou 1. Linka mezi R1-H a R2-C má přiřazenu cenu 10, i když by dle předpokladů měla mít linka cenu nižší (cena 1). Protože je na této lince umístěn rozbočovač, který pracuje s maximální rychlostí 10Mbit/s, má tato linka přiřazenou vyšší cenu 10. Z výpisu můžeme například vidět, že se ze směrovače R3-H do sítě 192.168.1.0, kde je umístěn PC1 dostaneme za cenu 2, jedná se o typ stub a oblast 0. Ve směrovací tabulce můžeme vidět informace pro všechny naše sítě.

Následující výpis je ze směrovače R2-C od firmy Cisco. Můžeme vidět směrovací tabulku od protokolu OSPF. Oproti výpisu ze zařízení Huawei jsou zde vypsány jen čtyři sítě, další dvě přímo připojené sítě Cisco nevypisuje. Pokud použijeme příkaz pro vypsání kompletní směrovací tabulky, jsou vidět všechny sítě, ať už přímo připojené nebo získané některým směrovacím protokolem. Při použití příkazu show ip ospf interface lze zjistit podrobné informace o rozhraních. Sériová linka s0/1/0 má opravdu přiřazenou cenu 781, rozhraní Fast Ethernet 0/0 má cenu 10. Z výpisu lze vidět jednotlivé sítě, za jakou cenu se k nim dostaneme a přes jaké rozhraní, písmeno „o“ zde znamená OSPF. Všechny jsou přes rozhraní Fa0/0 s adresou 10.0.0.1 je zde menší cena než přes sériovou linku s cenou 781. Například do sítě 192.168.2.0 se dostaneme za cenu 13.

```
R2-C#show ip route ospf 1

10.0.0.0/30 is subnetted, 4 subnets

O       10.0.0.4 [110/11] via 10.0.0.1, 00:44:14, FastEthernet0/0

O       10.0.0.12 [110/12] via 10.0.0.1, 00:43:19, FastEthernet0/0

O    192.168.1.0 [110/11] via 10.0.0.1, 00:45:09, FastEthernet0/0

O    192.168.2.0 [110/13] via 10.0.0.1, 00:43:19, FastEthernet0/0
```

Další výpisy a srovnání ze směrovačů Huawei a Cisco jsou přidány v příloze D. Během konfigurace směrovacího protokolu OSPF nebyly žádné problémy, ihned po konfiguraci směrovačů Huawei a Cisco vše fungovalo a problém s kompatibilitou zde žádný nebyl. Základní konfigurace na těchto zařízeních je velice podobná a liší se jen v maličkostech, ovšem výpisy jsou zde už rozdílnější.

6 Zabezpečená komunikace - IPSec VPN

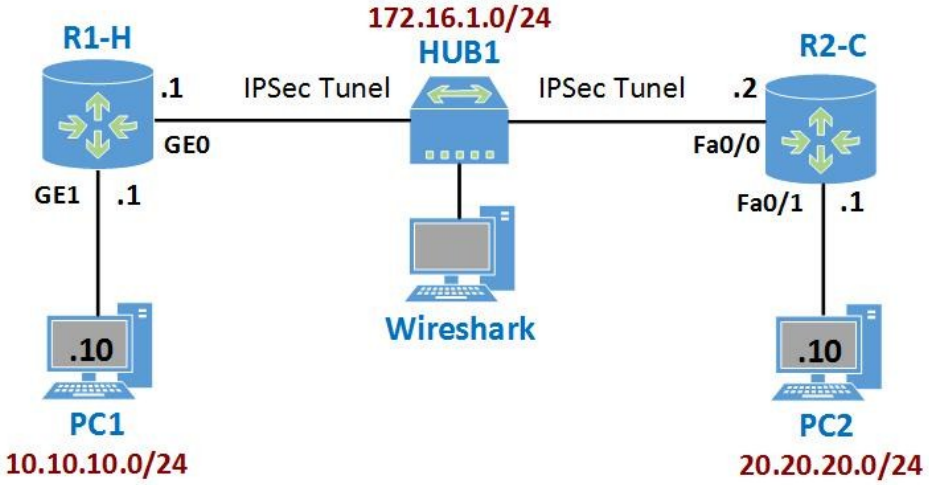
6.1 Základní popis IPSec VPN

IPsec (Internet Protocol Security) je standardizovaná skupina protokolů pro zajištění autentizace, integrity dat a šifrování IP komunikace mezi dvěma koncovými systémy, technicky realizovanou pomocí dynamicky navazovaných zabezpečených tunelů na síťové vrstvě referenčního modelu OSI/OSI RM, doplňuje IPv4 protokol (v IPv6 je povinnou součástí protokolu). IPSec jako první zařídí to, že se obě koncové strany navzájem identifikují (autentizují) a následně se šifruje komunikace pomocí domluveného algoritmu. IPSec není závislá na konkrétních algoritmech, neurčuje, jaké algoritmy se musí používat pro komunikaci. Definuje ale mechanismy vyjednávání a základní množinu algoritmů.

Skupinu parametrů dohodnutých pro šifrování a autentizaci mezi konci tunelu se nazývá Security Association (SA), v překladu bezpečnostní asociace. SA je v podstatě skupina algoritmů, které poskytují parametry pro bezpečnou komunikaci pomocí AH a ESP, obsahuje informaci o šifrovacích a autentizačních algoritmech a příslušné klíče. Pro každý směr provozu v tunelu je dohodnuto zvláštní SA s omezenou platností. Dohoda SA mezi konci tunelu se realizuje pomocí protokolu IKE (Internet Key Exchange), což je konkrétní implementace protokolu pro bezpečnou dohodu klíčů vyhovující obecnému rámci pro protokoly tohoto určení nazývanému ISAKMP (Internet Security Association and Key Management Protocol). Parametry pro autentizaci a šifrování jednotlivých paketů se přenášejí přímo v těchto paketech v pomocných hlavičkách, nazývaných Authentication Header (AH) a Encapsulating Security Payload (ESP). AH zajišťuje integritu a autentizaci zdroje dat, využívá hashovací funkce jako MD5 nebo SHA1 a společný klíč. ESP je novější a používanější hlavička, může zajistit všechny funkce jako AH a navíc ještě šifrování. Využívá šifrovací algoritmy jako DES nebo AES. IPSec může pracovat v jednom ze dvou režimů - transportním a tunelovém. Rozdíl mezi režimy je v tom, co se šifruje. Tunelový režim šifruje celý paket (včetně hlavičky) a doplňuje novou hlavičku. Transportní režim šifruje pouze data, IP hlavička se ponechá a doplní se pouze IPSec hlavička. [15]

6.2 Konfigurace

Na obrázku 4.3 lze vidět schéma zapojení sítě, které bylo použito při testování v laboratoři.



Obrázek 6.1: Schéma zapojení sítě pro IPSec

Pro vytvoření tunelu byly použity dva směrovače a mezi nimi připojen počítač se softwarem Wireshark pro sledování komunikace a zpráv. Při konfiguraci IPSec je důležité, aby na obou směrovačích byly nastaveny stejné parametry (šifrovací metoda, algoritmus pro ověření). Po správném nastavení IPSec, se mezi směrovači vytvoří šifrovaný tunel a pomocí softwaru Wireshak uvidíme již šifrovanou komunikaci. Důležité je také na směrovačích nastavit některý směrovací protokol nebo statické cesty, aby šlo komunikovat mezi počítači.

Konfigurace rozhraní – ukázka konfigurace rozhraní na směrovači R1, ostatní požadovaná rozhraní na směrovačích Huawei se nastaví stejným způsobem.

```
<R1-H> system-view
[R1-H] interface Gigabitethernet 0/0/0
[R1-H-GigabitEthernet0/0/0] ip address 172.16.1.0 24
[R1-H-GigabitEthernet0/0/0] quit
```

Konfigurace ACL – první nakonfigurujeme ACL list, zadáme zdrojovou a cílovou síť, na druhém směrovači jsou tyto sítě logicky naopak.

```
[R1-H] acl number 3101
[R1-H-acl-adv-3101] rule permit ip source 10.10.10.0 0.0.0.255 ->
                  -> destination 20.20.20.0 0.0.0.255
[R1-H-acl-adv-3101] quit
```

Konfigurace statické cesty – aby směrovače znaly všechny sítě, je potřeba nastavit do těchto sítí statickou cestu nebo použít některý ze směrovacích protokolů. Zde na směrovači Huawei můžeme vidět příkaz pro statickou cestu.

```
[R1-H] ip route-static 20.20.20.0 255.255.255.0 172.16.1.2
```

Konfigurace IKE proposal – IKE poskytuje automatickou ochranu distribuce klíčů, ověření identity a nastavení zabezpečené asociace SA. Pro použití a vyjednávání pomocí IKE je potřeba nakonfigurovat IKE Proposal (návrh) a IKE Peer. V IKE návrhu lze nastavit šifrovací algoritmus, algoritmus pro autentizaci, metodu ověřování při vyjednávání IKE, skupinu Diffie-Hellman pro výměnu klíčů, dále lze nastavit životnost SA.

```
[R1-H] ike proposal 1
[R1-H-ike-proposal-1] encryption-algorithm aes-cbc-128
[R1-H-ike-proposal-1] authentication-method pre-share
[R1-H-ike-proposal-1] authentication-algorithm sha1
[R1-H-ike-proposal-1] dh group2
[R1-H-ike-proposal-1] sa duration 86400
[R1-H-ike-proposal-1] quit
```

Konfigurace IKE peer – níže můžeme vidět základní konfiguraci IKE peer. V prvním příkazu si zvolíme název a verzi IKE peer. Následně nastavíme sdílený tajný klíč PSK (pre-shared key). Dalším příkazem zde zadáme již dříve vytvořený ike-proposal. Nakonec nastavíme IP adresu druhé komunikující strany (takzvaný peer), což je adresu rozhraní Fa0/0 směrovače R2-C.

```
[R1-H] ike peer PEER1 v1
[R1-H-ike-peer-PEER1] pre-shared-key test
[R1-H-ike-peer-PEER1] ike-proposal 1
[R1-H-ike-peer-PEER1] remote-address 172.16.1.2
```

Konfigurace IPSec proposal – jako poslední se musí nastavit IPSec proposal. V prvním příkazu si zvolíme název našeho ipsec proposal. V dalším příkazu transform zvolíme protokol ESP. Následně vybereme pro autentizaci SHA1 a pro šifrování AES. IPSec pracuje defaultně v tunelovém režimu, proto není potřeba tento režim nastavovat.

```
[R1-H] ipsec proposal PROPOSAL1
[R1-H-ipsec-proposal-PROPOSAL1] transform esp
[R1-H-ipsec-proposal-PROPOSAL1] esp authentication-algorithm sha1
[R1-H-ipsec-proposal-PROPOSAL1] esp encryption-algorithm aes-128
```

Konfigurace IPSec policy – když je IKE nakonfigurováno, můžeme jej aplikovat při vytvoření IPSec politiky. Zadáme zde i vytvořený ACL. Tuto vytvořenou mapu poté aplikujeme na požadované rozhraní.

```
[R1-H] ipsec policy map1 10 isakmp
[R1-H-ipsec-policy-isakmp-map1-10] ike-peer PEER1
[R1-H-ipsec-policy-isakmp-map1-10] proposal PROPOSAL1
[R1-H-ipsec-policy-isakmp-map1-10] security acl 3101
```

Konfigurace IPSec politiky na rozhraní – použití IPSec politiky na požadovaném rozhraní.

```
[R1-H] interface Gigabitethernet 0/0/0
[R1-H-GigabitEthernet0/0/0] ipsec policy map1
```

Příkazy pro kontrolu – zde je uvedeno několik příkazů pro kontrolu konfigurace a zobrazení informací o IPSec a IKE.

```
[R1-H]display ipsec proposal
[R1-H]display ipsec policy
[R1-H]display ipsec sa
[R1-H]display ike sa
[R1-H]display ike peer
```

Konfigurace směrovače Cisco je přiložena v příloze E. Jako zdroj pro konfiguraci směrovačů Huawei byla použita konfigurační příručka [16], kde lze nalézt také další konfigurační příkazy.

6.3 Ověření funkčnosti

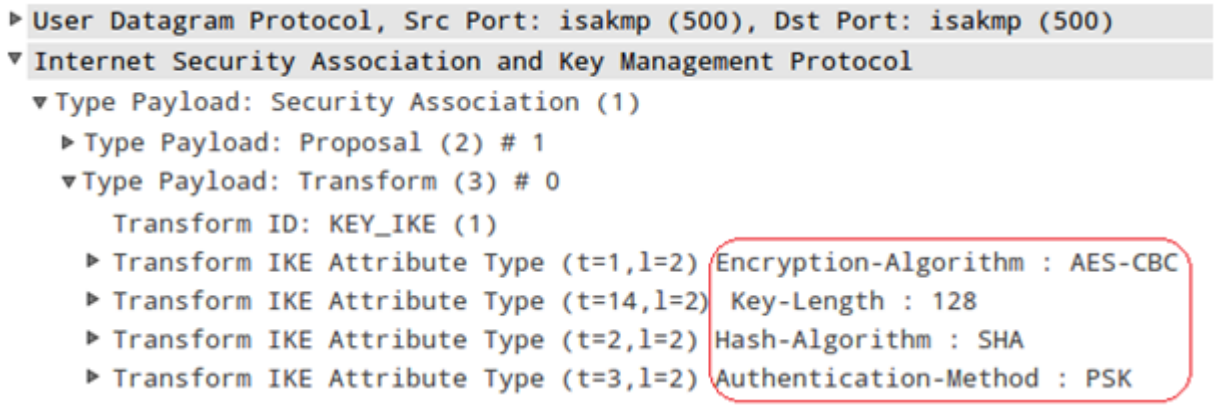
Na obrázku 6.2 lze vidět průběh počáteční komunikace a vyjednávání při vytváření IPSec tunelu mezi směrovači. Na začátku IPSec komunikace používá IKE (Internet Key Exchange) protokol pro vyjednání Security Association. IKE používá pro komunikaci UDP port 500 a pro autentizaci certifikáty nebo PSK (Pre-shared key). Pre-shared key (předem sdílený klíč) nebo PSK je sdílený tajný klíč, který je sdílen mezi oběma stranami prostřednictvím zabezpečeného kanálu. Naše nakonfigurovaná šifrovaná komunikace pomocí IPSec probíhá v takzvaném tunelovém režimu.

IKE pracuje ve dvou fázích, v první fázi se autentizují účastníci a vyjedná se IKE SA pomocí Diffie-Hellmanova protokolu, který je použit pro výměnu klíčů. Díky fázi jedna se vytvoří kanál pro vyjednání IPSec SA ve fázi dva. Fáze jedna pracuje v režimu Main nebo Aggressive Mode. Na obrázku lze vidět, že komunikace během první fáze probíhá v Main Mode režimu. Fáze dva vyjednává IPSec SA parametry a nastaví odpovídající bezpečnou asociaci SA. U této druhé fáze je použit pouze režim Quick Mode. [17]

Source	Destination	Protocol	Length	Info
172.16.1.1	172.16.1.2	ISAKMP	206	Identity Protection (Main Mode)
172.16.1.2	172.16.1.1	ISAKMP	130	Identity Protection (Main Mode)
172.16.1.1	172.16.1.2	ISAKMP	222	Identity Protection (Main Mode)
172.16.1.2	172.16.1.1	ISAKMP	298	Identity Protection (Main Mode)
172.16.1.1	172.16.1.2	ISAKMP	118	Identity Protection (Main Mode)
172.16.1.2	172.16.1.1	ISAKMP	118	Identity Protection (Main Mode)
172.16.1.1	172.16.1.2	ISAKMP	214	Quick Mode
172.16.1.2	172.16.1.1	ISAKMP	230	Quick Mode
172.16.1.1	172.16.1.2	ISAKMP	102	Quick Mode

Obrázek 6.2: Ukázka vyjednávání IPSec tunelu ze softwaru Wireshark

Na obrázku 6.3 je zobrazen výřez ze softwaru Wireshak, můžeme vidět UDP port 500, dále jsou zde zachyceny nastavené parametry při vyjednávání během první fáze. Použitý šifrovací algoritmus AES, délka klíče 128 bitů a autentizační metoda PSK.



Obrázek 6.3: Zachycené parametry při vyjednávání

Na obrázku 6.4 lze vidět zachycenou šifrovanou komunikaci, jedná se o ping počítače PC2 na počítač PC1. V tomto případě nelze vidět, o jaký typ zprávy se jedná, vidíme zdrojovou adresu, cílovou adresu a že se jedná o protokol ESP. Během vyjednávání se z parametrů SA naváže šifrovaná komunikace právě pomocí protokolu ESP.

Source	Destination	Protocol	Length	Info
172.16.1.2	172.16.1.1	ESP	166	ESP (SPI=0xa23c0103)
172.16.1.1	172.16.1.2	ESP	166	ESP (SPI=0x483174c1)

Obrázek 6.4: Zachycení zprávy Echo request, Echo reply

Po konfiguraci a úspěšné komunikaci mezi počítači PC1 a PC2 můžeme zkontrolovat všechna nastavení pomocí různých výpisů. V následující ukázce lze vidět ze směrovače Huawei příkaz display ike sa, kde vidíme adresu druhé komunikující strany. Parametry spojení RD a ST znamenají „ready“ a „stayalive“ v překladu tedy že peer je připraven a aktivní (naživu). Jako poslední také vidíme konkrétní fázi IKE protokolu.

```
[R1-H] display ike sa
     Conn-ID      Peer            VPN     Flag(s)      Phase
  -------------------------------------------------------------
       9          172.16.1.2      0       RD|ST        2
       7          172.16.1.2      0       RD|ST        1
```

Na směrovači Cisco je podobným příkazem show crypto isakmp sa, zde jsou vidět adresy zdroje a cíle, stav QM_IDLE, díky kterému víme, že tunel je připraven. Můžeme také vidět status ACTIVE. Navázání spojení mezi směrovači proběhlo bez problémů.

```
R2-C#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id   status
172.16.1.2      172.16.1.1      QM_IDLE        1001      ACTIVE
```

V příloze F jsou umístěny ostatní obsáhlejší výpisy ze směrovačů. U výpisu pro zobrazení je také důležité u příkazu zadat, zda chceme detailnější výpis, neboť výpisy se u směrovačů liší. V případě nenavázaní spojení se u IPSec u mnoha výpisu ani nezobrazí žádné informace a víme, že někde nastala chyba. Důležité je na obou směrovačích nastavit stejné parametry, IPSec tunel fungoval bez problémů jak s AES a SHA, tak i se starší MD5 a 3DES.

7 Technologie MPLS

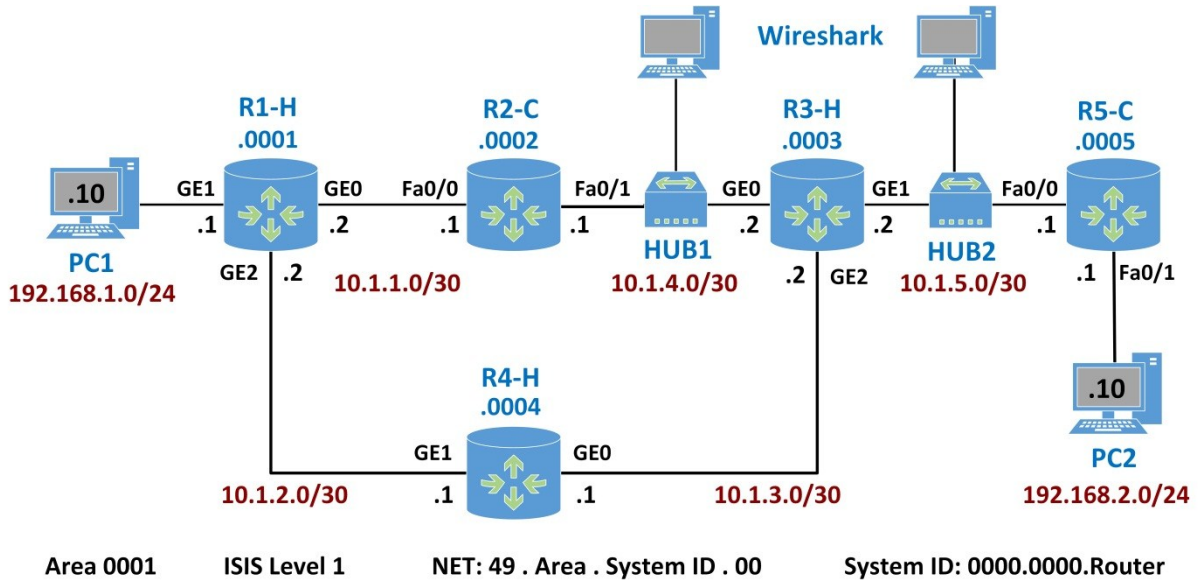
7.1 Základní popis MPLS

Technologie MPLS (MultiProtocol Label Switching) se používá pro urychlení cesty paketů sítí na principu přepínání značek. Je založený na důsledném oddělení procesu směrování (routing) od vlastního předávání paketů (forwarding). MPLS kombinuje techniku virtuálních kanálů s funkcemi z protokolového modelu TCP/IP. Toho je možné dosáhnout, protože jedno zařízení, označované jako LSR (Label Switch Router), hraje současně roli klasického IP směrovače a přepínače virtuálních kanálů. MPLS dokáže spolupracovat nejen s protokoly TCP/IP, ale i s protokoly z jiných modelů (např. IPX/SPX), také používá směrovací protokoly k zjištění topologie sítě.

Směrovač na okraji sítě s podporou MPLS se označuje jako LER (Label Edge Router). LER příchozímu paketu přidělí značku, která se pak dále používá pro jeho předávání mezi směrovači uvnitř MPLS sítě. LSR v síti pak mohou datagram předávat dál výhradně na základě svých individuálních jednoduchých tabulek se značkami, aniž by musely zkoumat své směrovací tabulky. Přepínací tabulky LSR směrovačů se vytvářejí pomocí signalizačního protokolu LDP (Label Distribution Protocol). Pomocí přepínacích tabulek LSR směrovačů LDP protokol vytváří virtuální cestu LSP (Label Switch Path). LSP je jednosměrný virtuální kanál. Pro přenos mezi dvěma LER směrovači je potřeba vytvořit alespoň dvě LSP, jednu pro každý směr. Jako u jiných technologií s virtuálními kanály má značka jen lokální význam. Když je paket přeposlán ze vstupního portu na výstupní, změní se hodnota jeho značky. Výstupní LER odebere značku a pošle IP paket do další sítě obvyklým způsobem. [18]

7.2 Konfigurace

V následující podkapitole je popsána základní konfigurace technologie MPLS a směrovacího protokolu IS-IS na zařízeních Huawei. Na obrázku 7.1 můžeme vidět zapojení sítě, které bylo použito při testování v laboratoři (včetně informací pro konfiguraci protokolu IS-IS). Rozhraní na směrovačích Huawei GE0/0/0, GE0/0/1, GE0/0/2 jsou pro přehlednost zkráceny na tvar GE0 atd. V zapojení byly použity tři směrovače Huawei a dva Cisco, do této sítě jsou umístěny dva rozbočovače s počítači pro odchyt komunikace pomocí softwaru Wireshark.



Obrázek 7.1: Schéma zapojení sítě pro MPLS

Při testování v laboratoři byly zapojeny do sítě nejprve čtyři směrovače, bez směrovače R4-H. Na směrovačích byl nakonfigurován směrovací protokol IS-IS a následně byla ověřena jeho funkčnost. Poté probíhalo nastavení a ověření MPLS. Nakonec byl do sítě přidán směrovač R4-H, aby se vytvořila další cesta pro komunikaci.

Konfigurace rozhraní – níže můžeme vidět ukázku konfigurace rozhraní na směrovači R1. Ostatní požadovaná rozhraní na směrovačích Huawei se nastaví stejným způsobem.

```
<R1-H> system-view
[R1-H] interface Gigabitethernet 0/0/0
[R1-H-GigabitEthernet0/0/0] ip address 10.1.1.2 30
[R1-H-GigabitEthernet0/0/0] quit
```

Konfigurace IS-IS – základní konfigurace protokolu IS-IS na směrovači R1. Druhý řádek konfigurace nastavuje směrovací proces na vnitro-oblastní. Další řádek konfigurace v rámci IS-IS reprezentuje přiřazení OSI NSAP adresy resp. NET identity, pod kterou bude směrovač v rámci konfigurovaného IS-IS procesu vystupovat. Nakonec na požadovaných rozhraních zapneme nakonfigurovaný protokol IS-IS. Tímto způsobem provedeme konfiguraci na zbývajících směrovačích. Více informací o protokolu IS-IS se lze dočíst zde. [19] [20]

```
[R1-H] isis 1
[R1-H-isis-1] is-level level-1
[R1-H-isis-1] network-entity 49.0001.0000.0000.0001.00
[R1-H-isis-1] quit
[R1-H] interface GigabitEthernet 0/0/0
[R1-H-GigabitEthernet0/0/0] isis enable 1
```

Konfigurace MPLS – základní konfigurace MPLS na směrovači R1. Jako první je potřeba manuálně nastavit LSR ID, jinak není umožněna konfigurace MPLS. Oproti Cisco směrovači je toto rozdílné - Cisco si na LSR ID přiřadí automaticky adresu ze sítě. Doporučuje se, aby na LSR ID byla použita adresa loopbacku, při konfiguraci byly ovšem použity normální adresy ze sítě. Poté následuje zapnutí funkce MPLS a MPLS LDP. Nakonec musíme na požadovaném rozhraní funkci MPLS povolit. Tímto způsobem provedeme konfiguraci na zbývajících směrovačích.

```
[R1-H] mpls lsr-id 192.168.1.1
[R1-H] mpls
[R1-H-mpls] quit
[R1-H] mpls ldp
[R1-H-mpls-ldp] quit
[R1-H] interface Gigabitethernet 0/0/0
[R1-H-GigabitEthernet0/0/0] mpls
[R1-H-GigabitEthernet0/0/0] mpls ldp
[R1-H-GigabitEthernet0/0/0] quit
```

Konfigurace hello, keepalive – níže lze vidět příklad konfigurace časovačů pro spojení LDP. Jedná se o hello send a hello hold intervaly, tyto intervaly se zadávají v sekundách. Stejným příkazem se nastaví také keepalive, v příkazu se změní pouze hello na keepalive.

```
[R1-H] interface Gigabitethernet 0/0/0
[R1-H-GigabitEthernet0/0/0] mpls ldp timer hello-send interval
[R1-H-GigabitEthernet0/0/0] mpls ldp timer hello-hold interval
```

Příkazy pro kontrolu – zde jsou uvedeny některé příkazy pro kontrolu konfigurace a zobrazení informací o MPLS, například zobrazení spojení, zobrazení sousedů a rozhraní.

```
[R1-H]display mpls ldp session
[R1-H]display mpls route-state
[R1-H]display mpls ldp peer
[R1-H]display mpls ldp interface
```

Konfigurace směrovače Cisco je přiložena v příloze G. Jako zdroj pro konfiguraci směrovačů Huawei byly použity konfigurační příručky [14] [21], kde lze nalézt další konfigurace.

7.3 Ověření funkčnosti

Na obrázku 7.2 lze vidět průběh komunikace LDP ze softwaru Wireshark, jedná se o komunikaci mezi směrovači R3-H a R5-C. Můžeme vidět zasílání zpráv Hello, které se v časových intervalech posílají na adresu 224.0.0.2. Dále je vidět komunikaci mezi směrovači, ty zde vystupují pod svým nastaveným lsr-id. Ze začátku si směrovače pošlou inicializační zprávy. Další typ zprávy, který se posílá v časových intervalech je Keep alive.

Source	Destination	Protocol	Length	Info
10.1.5.2	224.0.0.2	LDP	76	Hello Message
10.1.5.1	224.0.0.2	LDP	76	Hello Message
192.168.2.1	10.1.5.2	LDP	90	Initialization Message
10.1.5.2	192.168.2.1	LDP	98	Initialization Message
10.1.5.2	192.168.2.1	LDP	86	Address Message
10.1.5.2	192.168.2.1	LDP	97	Label Mapping Message
10.1.5.1	224.0.0.2	LDP	76	Hello Message
10.1.5.2	224.0.0.2	LDP	76	Hello Message
192.168.2.1	10.1.5.2	LDP	72	Keep Alive Message
10.1.5.2	192.168.2.1	LDP	72	Keep Alive Message

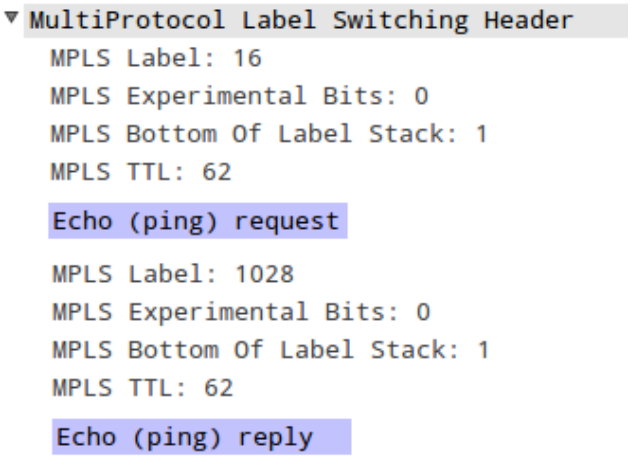
Obrázek 7.2: Ukázka komunikace ze softwaru Wireshark

Na obrázku 7.3 lze vidět zachycenou komunikaci (HUB1), jedná se o ping počítače PC2 na počítač PC1. Vidíme zdrojovou adresu, cílovou adresu, a že se jedná o protokol ICMP. Na obrázku 7.4 lze vidět zachycené informace o MPLS, v prvním případě se jedná o informace požadavku (request) a poté o informace odpovědi (reply). První parametr, který můžeme na obrázku 7.4 vidět je značka (MPLS Label). Tato značka (label) se používá při výběru odpovídající LSP. Parametr experimental původně sloužil pro budoucí využití. Nyní ho lze použít k specifikaci třídy provozu vyžadující určitou úroveň kvality služby. Další parametr Bottom of Label Stack indikuje poslední MPLS záhlaví v řadě,

pokud je jich použito více. Poslední parametr TTL (Time to live) má stejnou funkci jako stejnojmenné pole v záhlaví IP paketu. Určitě si lze všimnout velkého rozdílu hodnot u značky (Label) pro odchozí a příchozí zprávu. Cisco směrovač přiřazuje hodnoty postupně, v tomto případě má značka hodnotu 16. Huawei přiřazuje hodnoty značek vyšší, od tisíce a postupně zvyšuje. Příchozí odpověď měla hodnotu značky 1028. Odchyt komunikace byl proveden uprostřed sítě mezi směrovači R2-C a R3-H. Kdyby byla komunikace sledována na rozbočovači HUB2, příchozí odpověď by již značku neměla. Předposlední směrovač v cestě totiž značku odstraní.

Source	Destination	Protocol	Length	Info
192.168.2.10	192.168.1.10	ICMP	102	Echo (ping) request
192.168.1.10	192.168.2.10	ICMP	102	Echo (ping) reply

Obrázek 7.3: Zachycený ping z PC2 na PC1



Obrázek 7.4: Zachycené informace MPLS

V následující ukázce můžeme vidět výpis jednoho, ze základních příkazů pro ověření MPLS. Příkaz display mpls ldp session zobrazí navázaná spojení. Jedno spojení má PeerID 10.1.3.1 a druhé spojení má PeerID 10.1.4.1. Můžeme zde vidět parametr status, který nám říká, že spojení je funkční (Operational). Díky parametru SSnRole můžeme vidět roli současného LSR zařízení, která je aktivní (Active). Poslední parametr KASent/Rcv zobrazuje počet odeslaných a přijatých zpráv KeepAlive.

```
[R1-H] display mpls ldp session

LDP Session(s) in Public Network

Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)

A '*' before a session means the session is being deleted.

------------------------------------------------------------------

PeerID          Status       LAM  SsnRole  SsnAge       KASent/Rcv

------------------------------------------------------------------

10.1.3.1:0      Operational  DU   Active   0000:00:23   94/94

10.1.4.1:0      Operational  DU   Active   0000:01:27   352/400

------------------------------------------------------------------
```

V následující ukázce můžeme vidět výpis příkazu display mpls lsp ze směrovače R1-H. Tento příkaz nám zobrazí základní informace o LSP. V tomto výpisu jsou vidět výstupní, případně vstupní rozhraní do konkrétní sítě, která není přímo připojena do směrovače. Dále můžeme vidět přiřazenou vstupní a výstupní značku (label), lze si všimnout, že Huawei opravdu přiřazuje značky vyšších hodnot. Do sítě 192.168.2.0 vedou dvě cesty. Jedna cesta vede přes rozhraní GE0/0/0, kde je next hop směrovač Cisco R2-C, další cesta vede přes rozhraní GE0/0/2 a následuje směrovač Huawei R4-H. V tomto výpisu jsou vidět jen základní informace, pro obsáhlejší výpis pak slouží například příkaz display mpls ldp lsp, kde můžeme vidět kompletní LDP LSP informace. V příloze H jsou umístěny ostatní výpisy ze směrovačů jak pro funkci MPLS tak směrovací protokol IS-IS.

```
[R1-H]display mpls lsp
------------------------------------------------------------
LSP Information: LDP LSP
------------------------------------------------------------
FEC                 In/Out Label        In/Out IF      Vrf Name
10.1.4.0/30         1029/3              -/GE0/0/0
10.1.5.0/30         1033/17             -/GE0/0/0
192.168.2.0/24      1034/18             -/GE0/0/0
192.168.2.0/24      1034/1031           -/GE/0/0/2
```

8 Podpora protokolu IPv6

8.1 Základní popis IPv6 a BGP

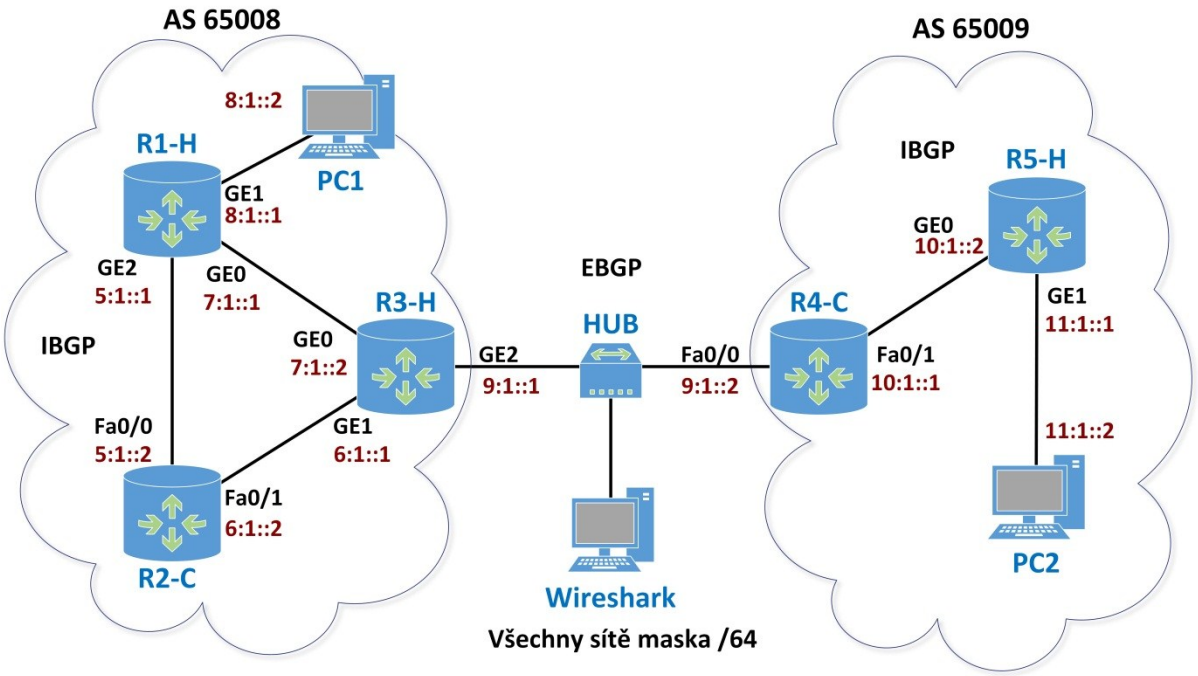
Následující podkapitola obsahuje ověření funkčnosti a kompatibility internetového protokolu IPv6 mezi směrovači Huawei a Cisco. IP verze 6 neboli IPv6 je nástupcem stávajícího IP protokolu (označované jako IPv4). Přináší zejména masivní rozšíření adresního prostoru. Počet IPv4 adres je 2^{32}, kdežto IPv6 adres je 2^{128}. Bohužel IPv6 není zpětně kompatibilní s IPv4. Musí se proto zavádět souběžně k IPv4 tak, aby uživatelům vše fungovalo. Plný zápis IPv6 adresy je osm čtveřic hexadecimálních číslic oddělených dvojtečkou. Více o IPv6 protokolu se lze dočíst zde [22].

Směrovací protokol BGP (Border Gateway Protocol) je protokol pro směrování mezi autonomními systémy (AS). Pomocí BGP si hraniční směrovače vyměňují informace o sítích v jednotlivých autonomních systémech a o tom, přes které autonomní systémy se lze k jednotlivým sítím dostat. BGP nepracuje s grafem propojení jednotlivých směrovačů a sítí, ale s grafem propojení autonomních systémů. V tomto grafu jsou pak vyhledávány cesty mezi sítěmi v různých autonomních systémech. Na rozdíl od vnitřních směrovacích protokolů nemá BGP jednoznačnou metriku, podle níž by za všech okolností automaticky volil nejkratší cesty do jednotlivých cílových sítí. Při směrování mezi AS totiž směrujeme provoz přes cizí AS, jejichž provozovatelé mají nejrůznější zájmy a podmínky. Respektováním všech těchto faktorů pak určíme tzv. směrovací politiku.

Protokol BGP bývá někdy označován jako protokol speciální třídy, nazývané path-vector. Path vector je potom posloupnost čísel autonomních systémů, přes které vede cesta k nějaké síti. Protože cesta nesmí obsahovat smyčku, může se číslo autonomního systému v path vector objevit nejvýše jednou. Path vector také slouží k výběru nejkratší cesty do jednotlivých sítí. [23]

8.2 Konfigurace

Na obrázku 8.1 lze vidět reálné zapojení sítě, které bylo použito při testování v laboratoři.



Obrázek 8.1: Schéma zapojení sítě pro BGP – IPv6

V následující podkapitole je popsána základní konfigurace IPv6 a směrovacího protokolu BGP s podporou IPv6. Na obrázku 8.1 lze vidět, že rozhraní na směrovačích Huawei GE0/0/0, GE0/0/1, GE0/0/2 jsou pro přehlednost zkráceny na tvar GE0 atd. V zapojení bylo použito celkem 5 směrovačů (tři Huawei a dva Cisco), jeden rozbočovač pro odchyt komunikace mezi autonomními systémy AS 65008 a AS 65009 pomocí software Wireshark. Všechny sítě mají masku /64 a jsou zapsány ve zkráceném tvaru. Více o IPv6 adresách a zkracování zápisu se lze dočíst zde [22]. U protokolu BGP se také můžeme setkat s vazbou EBGP a IBGP. Vazbu mezi BGP směrovači v různých AS nazýváme externí BGP (EBGP), zde se jedná o vazbu mezi směrovači R3-H a R4-C. Vazba mezi BGP směrovači v tomtéž AS je potom interní BGP (IBGP), na obrázku 8.1 se jedná o vazby mezi směrovači v levém AS 65008 a pravém AS 65009.

Konfigurace rozhraní – níže můžeme vidět konfiguraci rozhraní GE 0/0/0 na směrovači R1-H. Jako první příkaz v systémovém režimu zadáme pouze ipv6, tento příkaz zapíná podporu IPv6. Pokud chceme pracovat s IPv6 tento příkaz musíme vždy zadat. Poté vybereme požadované rozhraní a na něm povolíme IPv6 pomocí příkazu ipv6 enable. V případě že bychom nezapnuli IPv6 v systémovém režimu, směrovač nás na to upozorní. Nakonec nastavíme odpovídající IPv6 adresu.

```
<R1-H> system-view
[R1-H] ipv6
[R1-H] interface Gigabitethernet 0/0/0
[R1-H-GigabitEthernet0/0/0] ipv6 enable
[R1-H-GigabitEthernet0/0/0] ipv6 address 7:1:1 64
[R1-H-GigabitEthernet0/0/0] quit
```

Konfigurace BGP – níže je uvedena konfigurace směrovacího protokolu BGP na směrovači R3-H. Prvním příkazem se dostaneme do režimu směrovacího protokolu, zadáme požadované číslo AS. V tomto režimu jako první nastavíme id směrovače na 3.3.3.3 (ostatní směrovače mají id podle jejich čísla označení, např. R2 – 2.2.2.2). Každé dva směrovače, které mají navázané spojení, se nazývají sousedé nebo peers. Dalším příkazem tedy nastavím adresu souseda, a že se nachází ve stejném AS – 65008. Po nakonfigurování souseda v BGP režimu, ho musíme povolit v BGP IPv6. Použijeme příkaz ipv6-family unicast a v následujícím režimu souseda povolíme. Poslední příkaz musíme zadat pro přidání sítě, která je mezi našimi směrovači. Zde při zadávání příkazu nás může zaskočit výpis směrovače, že zadaná síť neexistuje. Tento výpis se zobrazí v případě, že naše rozhraní, na kterém se nachází síť je ve stavu „down“ a není aktivní. Poté, co je rozhraní a linka mezi směrovači již aktivní, příkaz lze zadat bez problémů. Tímto způsobem provedeme konfiguraci na ostatních směrovačích, kde zadáme požadované sousedy.

```
[R3-H] bgp 65008
[R3-H-bgp] router-id 3.3.3.3
[R3-H-bgp] peer 7:1::1 as-number 65008
[R3-H-bgp] ipv6-family unicast
[R3-H-bgp-af-ipv6] peer 7:1::1 enable
[R3-H-bgp-af-ipv6] network 7:1:: 64
[R3-H-bgp-af-ipv6] quit
```

V následující ukázce můžeme vidět opět zprovoznění vazby na směrovači R3 a to konfiguraci EBGP vazby ke směrovači R4-C. Podrobný popis konfigurace již byl popsán a zde se postupuje stejně. Je zde rozdíl pouze při zadávání čísla AS u nastavení adresy souseda. V tomto případě se směrovač R4-C nachází v jiném AS (65009).

```
[R3-H] bgp 65008
[R3-H-bgp] peer 9:1::2 as-number 65009
[R3-H-bgp] ipv6-family unicast
[R3-H-bgp-af-ipv6] peer 9:1::2 enable
[R3-H-bgp-af-ipv6] network 9:1:: 64
[R3-H-bgp-af-ipv6] quit
```

Konfigurace protokolu IPv6 a směrovacího protokolu BGP směrovače Cisco je umístěna v příloze I. Jako zdroj pro konfiguraci směrovačů Huawei byla použita konfigurační příručka [24], kde lze nalézt další konfigurace.

8.3 Ověření funkčnosti

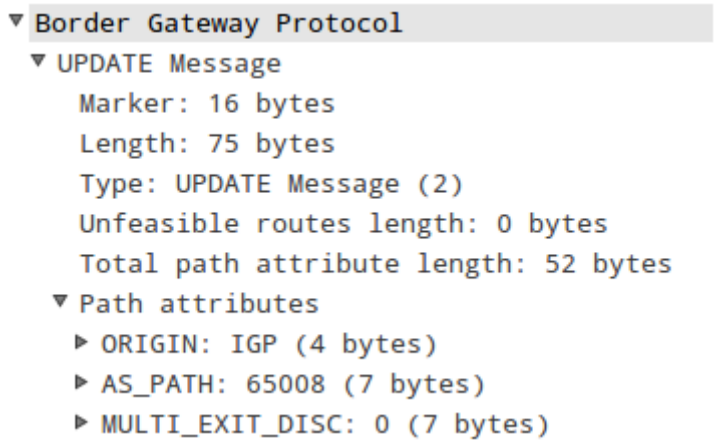
Na obrázku 8.2 můžeme vidět průběh komunikace protokolu BGP ze softwaru Wireshark, jedná se o komunikaci mezi směrovači R3-H a R4-C. Směrovací informace se v BGP vyměňuje vždy mezi sousedními směrovači. O tom, které směrovače budou sousedy, rozhoduje administrátor při konfiguraci BGP. Výměna směrovacích informací mezi sousedy probíhá s použitím protokolu TCP na portu 179, jedná se tedy o spolehlivé spojení. Po navázání spojení mezi sousedy se vymění kompletní směrovací informace.

Existují 4 typy zpráv, které si mezi sebou sousedé vyměňují. První zprávou posílanou mezi sousedy je zpráva Open. Zpráva Open je vyměňovaná při zřizování vazby mezi sousedními směrovači. V této zprávě se například vyjedná verze používaného protokolu BGP a sousední směrovače se také informují o číslech AS, do kterých patří. Další parametr, který se ve zprávě Open dohodne je například interval HoldTime. Pro výměnu směrovacích informací mezi sousedy je určena zpráva Update, tato zpráva nese samotné směrovací informace. Může zde být proměnný počet tzv. atributů, které jsou společně přiřazeny všem uvedeným cestám. Zpráva Keepalive se posílá periodicky pro ověření funkčnosti linky. Typicky se vysílá v intervalu 60 sekund. Spojení se považuje za nefunkční, pokud od souseda nepřišla zpráva Keepalive po dobu HoldTime dohodnutou pomocí zprávy Open. Zpráva Notification indikuje chybu v činnosti BGP. Po vyslání této zprávy dojde k ukončení vazby mezi sousedy rozpojením TCP spojení.

Source	Destination	Protocol	Length	Info
9:1::1	9:1::2	BGP	119	OPEN Message
9:1::2	9:1::1	BGP	119	OPEN Message
9:1::1	9:1::2	BGP	93	KEEPALIVE Message
9:1::2	9:1::1	BGP	256	UPDATE Message, UPDATE Message
9:1::2	9:1::1	BGP	93	KEEPALIVE Message
9:1::1	9:1::2	BGP	149	UPDATE Message

Obrázek 8.2: Ukázka komunikace BGP ze softwaru Wireshark

Na obrázku 8.3 je zobrazen výřez ze softwaru Wireshark zachycené zprávy Update. Abychom byli schopni explicitně ovlivňovat směrovací politiky, je potřebný mechanismus, kterým bychom vyjádřili preferenci, resp. zákaz některých cest podle nejrůznějších kritérií. K tomuto účelu v protokolu BGP slouží právě atributy, které můžeme každému záznamu o cestě k cílové síti přiřadit. Na obrázku 8.3 můžeme vidět některé z atributů. První atribut ORIGIN říká, odkud se informace o cestě v BGP vzala. Může nabývat hodnot IGP (cesta pochází z vnitřního směrovacího protokolu), EGP (cesta získána redistribucí z externího směrovacího protokolu EGP) nebo INCOMPLETE (původ cesty není znám). Druhý zachycený atribut AS_PATH je povinný atribut (tzv. well-known mandatory), musí být tedy povinně uveden u každé cesty. Obsahuje postupně řetězec čísel autonomních systémů, přes které vede cesta k cílové síti. Atribut MULTI_EXIT_DISC (Multiple Exit Discriminator) je nepovinný atribut (tzv. optional non-transitive) informuje externí sousedy o preferované cestě do AS, které má více vstupních cest. Více o atributech a jejich vyhodnocování se lze dočíst zde [23].



Obrázek 8.3: Zachycené atributy zprávy Update

V následující ukázce můžeme vidět výpis příkazu show bgp ipv6 ze směrovače R3 od firmy Cisco. Po zadání příkazu lze vidět jednotlivé sítě, jejich next hop a další parametry pro BGP jako například Weight a Path. Vysvětlení jednotlivých znaků bude, pospáno na další straně.

```
R2-C#show bgp ipv6
     Network          Next Hop    Metric     LocPrf       Weight     Path
*>   5:1::/64         ::               0                    32768     i
* i                   5:1::1           0        100             0     i
* i  6:1::/64         6:1::1           0        100             0     i
*>                    ::               0                    32768     i
* i  7:1::/64         6:1::1           0        100             0     i
*>i                   5:1::1           0        100             0     i
*>i  8:1::/64         5:1::1           0        100             0     i
*>i  9:1::/64         6:1::1           0        100             0     i
*>i10:1::/64          9:1::2           0        100             0     65009 i
*>i11:1::/64          9:1::2           0        100             0     65009 i
```

První tři znaky před sítí značí statusy (status code), tyto znaky jsou totožné s těmi, které používají směrovače Huawei, viz výpis níže od směrovače Huawei. Znak * *(valid)* znamená, že je síť v tabulce validní. Znak > *(best)* znamená, že je tuto položku nejlepší použít pro vstup této sítě. Další znak *i (internal)* znamená, že záznam v tabulce byl naučen přes interní BGP (IBGP) spojení. U parametru Path (Origin) znak *i* znamená, že vstup pochází z protokolu IGP (Interior Gateway Protocol). Z výpisu lze například vidět u sítě 10:1::/64, že je použit Next hop 9:1::2, což je IP adresa systému, který se používá při předávání paketů k cílové síti. Jako poslední můžeme vidět parametr Path, který zobrazuje autonomní systém cesty do cílové sítě.

Na dalším výpisu můžeme vidět příkaz display bgp ipv6 routin g-table ze směrovače R5-H. Je zde zobrazen jen úsek toho výpisu (dvě sítě), neboť výpis je obsáhlý. Kompletní výpis je umístěn v příloze J. Můžeme zde vidět podobný výpis jako ze směrovače Cisco, jen jinak uspořádaný. Nachází se zde všechny již výše popsané parametry. Lze například vidět, že do sítě 5:1::/64 vede cesta přes Next hop 9:1::1 a tato síť se nachází v autonomním systému AS 65008.

```
[R5-H]display bgp ipv6 routing-table
 BGP Local router ID is 5.5.5.5
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 8
 *>i Network  : 5:1::                                PrefixLen : 64
     NextHop  : 9:1::1                               LocPrf    : 100
     MED      : 0                                    PrefVal   : 0
     Label    :
     Path/Ogn : 65008 i
 *>i Network  : 9:1::                                PrefixLen : 64
     NextHop  : 10:1::1                              LocPrf    : 100
     MED      : 0                                    PrefVal   : 0
     Label    :
     Path/Ogn : i
```

Další výpisy ze směrovačů Huawei a Cisco jsou umístěny v příloze J. Po konfiguraci směrovačů Huawei a Cisco vše fungovalo a problém s IPv6 kompatibilitou žádný nebyl, fungovaly jak směrovací protokoly, tak statické cesty. Aby bylo možné s IPv6 pracovat je nutné na každém směrovači zapnout podporu IPv6 směrování (při nezapnutí směrovač vypíše upozornění).

9 Závěr

V rámci své bakalářské práce jsem v jednotlivých kapitolách splnil cíle, které byly určeny. V úvodní kapitole jsem se zaměřil na zařízení od společnosti Huawei. Stručně jsem zde popsal jejich parametry a rozdělní jednotlivých řad. Po seznámení se směrovači Huawei, jak po technické, tak po praktické stránce, jsem porovnal směrovač Huawei AR2220 se směrovačem Cisco 2801. Ze směrovačů, které jsem měl k dispozici, jsou tyto dva svými parametry nejvíce podobné. Po celkovém přehledu směrovačů jsem začal pracovat na hlavním úkolu této práce a to praktickém testování funkcí na směrovačích.

V praktické části jsem jako první funkci pro testování vybral směrovací protokol OSPF. Směrovací protokol je jedna ze základních funkcí směrovačů. Při testování směrovacího protokolu OSPF mezi směrovači obou výrobců nedošlo k problémům s kompatibilitou a funkčností. Postup konfigurace mezi směrovači byl velice podobný. Druhou funkcí, která byla testována, je vytvoření zabezpečené komunikace pomocí IPSec VPN. Zde mezi směrovači již byly při konfiguraci rozdíly. Parametry IPSec pro konfiguraci směrovačů byly stejné, ale způsob nastavení a postup zadávání konfigurace byl rozdílnější. Další testovanou funkcí byla technologie MPLS. U této funkce bylo potřeba v zapojené síti použít některý směrovací protokol. Zde jsem použil méně častý směrovací protokol IS-IS. U směrovačů jsem provedl základní konfiguraci MPLS a následně ověřil funkčnost a kompatibilitu. Poslední funkcí, kterou jsem testoval, byla podpora protokolu IPv6. Při konfiguraci všech testovaných funkcí mezi směrovači Huawei a Cisco nedošlo k problému s kompatibilitou. Důležité je říci, že záleží na verzi operačního systému směrovačů. Během testování byl dodán nový firmware od výrobce Huawei, díky kterému byly k dispozici například zcela nové konfigurační příkazy.

U většiny výrobců bývá prostředí a syntaxe příkazu velmi podobné. U směrovačů Huawei a Cisco jsou některé konfigurační příkazy naprosto totožné. Většina konfiguračních příkazů je si dosti podobná. Co se týče konfiguračního prostředí, je zde mezi směrovači určitý rozdíl v logice konfiguračních režimů. Dle mého vlastního názoru mají směrovače od obou výrobců své vlastní výhody. Co se týče přehlednosti konfigurace, u směrovačů Huawei mi přišel postup a rozčlenění konfigurace například u IPSec do několika konfiguračních „podrežimů“ přehlednější a přívětivější. U jiných konfigurací tomuto bylo zase naopak. Dalším mým postřehem během testování je rozdílná doba startu směrovačů. Směrovače Huawei při zapnutí nabíhaly výrazně déle než směrovače Cisco 2801. Také rozšiřovací karty pro směrovače jsou velikostně rozdílné. Karty pro směrovač Cisco 2801 jsou o mnoho menší než pro Huawei.

Hlavním přínosem této bakalářské práce pro mne byla možnost vyzkoušet zařízení jiného výrobce než kterého znám. Díky práci jsem se seznámil se směrovači Huawei a jejich konfigurací. Tuto zkušenost beru jako výhodu a praxi do budoucna v oblasti počítačových sítí. Přínos této bakalářské práce v oboru počítačových sítí vidím v tom, že byla ověřena kompatibilita testovaných funkcí mezi směrovači těchto dvou výrobců. Dalším přínosem je například fakt, že informace a konfigurace směrovačů Huawei jsou přeloženy do českého jazyka, neboť veškerá dokumentace ke směrovačům Huawei jsou v anglickém jazyce. Pro toho, kdo se chce věnovat této problematice, může mu do začátku tato práce sloužit jako přehled informací a návod na konfiguraci již zmíněných testovaných funkcí na směrovačích Huawei.

Použitá literatura

[1] AR3200 Series Routers Brochure. *AR3200 - Huawei Products* [online]. [cit. 2013-04-04]. Dostupné z: http://www.huawei.com/ucmf/groups/public/documents/attachments/hw_093992.pdf

[2] AR2200 Series Routers Brochure. *AR2200 - Huawei Products* [online]. [cit. 2013-04-04]. Dostupné z: http://www.huawei.com/ucmf/groups/public/documents/attachments/hw_093991.pdf

[3] AR1200 Series Routers Brochure. *AR1200 - Huawei Products* [online]. [cit. 2013-04-04]. Dostupné z: http://www.huawei.com/ucmf/groups/public/documents/attachments/hw_093990.pdf

[4] AR3200 Series Enterprise Routers. *Huawei Enterprise - Routers* [online]. [cit. 2013-04-04]. Dostupné z: http://enterprise.huawei.com/en/products/network/Routers/ar-g3/hw-201685.htm

[5] AR2200 Series Enterprise Routers. *Huawei Enterprise - Routers* [online]. [cit. 2013-04-04]. Dostupné z: http://enterprise.huawei.com/en/products/network/Routers/ar-g3/hw-201687.htm

[6] AR1200 Series Enterprise Routers. *Huawei Enterprise - Routers* [online]. [cit. 2013-04-04]. Dostupné z: http://enterprise.huawei.com/en/products/network/Routers/ar-g3/hw-201692.htm

[7] ZLOCH, Tomáš. Prezentace Huawei Networking. *Huawei Technologies* [online]. [cit. 2013-04-03]. Dostupné z: http://www.datainter.cz/doc/DTDXIX/DTDXIX_Huawei.pdf

[8] Cisco 2800 Integrated Services Routers. *Data Sheet* [online]. [cit. 2013-04-04]. Dostupné z: http://www.cisco.com/en/US/prod/collateral/routers/ps5854/ps5882/product_data_sheet0900aecd8016fa68_ps5854_Products_Data_Sheet.html

[9] Cisco Router Guide. *Cisco 2800 Routers Brochures* [online]. [cit. 2013-04-04]. Dostupné z: http:/www.cisco.com/en/US/prod/collateral/routers/ps5855/prod_brochure0900aecd8019dc1f.pdf

[10] Cisco 2800 Series Routers Models Comparison 2801 2811 2821 2851. *Router-Switch.com* [online]. [cit. 2013-04-04]. Dostupné z: http://www.router-switch.com/cisco-2800-series-routers-models-comparison-2801-2811-2821-2851-pd-45.html

[11] Product Views. *Cisco 2801 Integrated Services Router* [online]. [cit. 2013-04-04]. Dostupné z: http://www.cisco.com/en/US/products/ps6018/prod_view_selector.html

[12] AR150&AR200&AR1200&AR2200&AR3200 V200R003C00 Configuration Guide-Basic Configuration 02. *Enterprise Service Support - AR* [online]. [cit. 2013-04-04]. Dostupné z: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000009824&idPath=7919710|9856750|7923148|9858988|6078842

[13] GRYGÁREK, Petr. Směrovací protokol OSPF. *Směrované a přepínané sítě* [online]. [cit. 2013-04-04]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/OSPF/ospf.html

[14] AR150&AR200&AR1200&AR2200&AR3200 V200R003C00 Configuration Guide-IP Routing 02. *Enterprise Service Support - AR* [online]. [cit. 2013-04-04]. Dostupné z: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000009828&idPath=7919710|9856750|7923148|9858988|6078842

[15] GRYGÁREK, Petr. Bezpečnost počítačových sítí. *Směrované a přepínané sítě* [online]. [cit. 2013-04-04]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/bezpecnost-ucitele.pdf

[16] AR150&AR200&AR1200&AR2200&AR3200 V200R003C00 Configuration Guide-VPN 02. *Enterprise Service Support - AR* [online]. [cit. 2013-04-04]. Dostupné z: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000009839&idPath=7919710|9856750|7923148|9858988|6078842

[17] VPN 1 - IPsec VPN a Cisco. *SAMURAJ-cz.com* [online]. [cit. 2013-04-04]. Dostupné z: http://www.samuraj-cz.com/clanek/vpn-1-ipsec-vpn-a-cisco/

[18] MACHNÍK, Petr. Přednáška IP WAN sítě. *Předmět Telekomunikační sítě*, [cit. 2012-03-05]. Dostupné z: http://moodle.kat440.vsb.cz/

[19] MILATA, Martin. Protokol IS-IS. *MilataWiki* [online]. [cit. 2013-04-05]. Dostupné z: http://wh.cs.vsb.cz/mil051/index.php/Sm%C4%9Brovac%C3%AD_protokol_IS-IS_(Intermediate_System-to-Intermediate_System_Protocol)

[20] Cisco Routing 4 - IS-IS - Intermediate System to Intermediate System. *SAMURAJ-cz.com* [online]. [cit. 2013-04-05]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-routing-4-is-is-intermediate-system-to-intermediate-system/

[21] AR150&AR200&AR1200&AR2200&AR3200 V200R003C00 Configuration Guide-MPLS 02. *Service Support - AR* [online]. [cit. 2013-04-05]. Dostupné z: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000009832&idPath=7919710|9856750|7923148|9858988|6078842

[22] Vlastnosti protokolu IPv6. *Co je IPv6 – IPv6.cz* [online]. [cit. 2013-04-12]. Dostupné z: https://www.ipv6.cz/Co_je_IPv6

[23] GRYGÁREK, Petr. Směrovací protokol BGP. *Směrované a přepínané sítě* [online]. [cit. 2013-04-12]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html

[24] AR150&AR200&AR1200&AR2200&AR3200 V200R002C02 Configuration Guide - IP Routing 01. *Service Support - AR* [online]. [cit. 2013-04-12]. Dostupné z: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000005091&idPath=7919710|9856750|7923148|9858988|6078842

[25] AR150&AR200&AR1200&AR2200&AR3200 Product Documentation – Technical specifications. *Product Service Support - AR* [online]. [cit. 2013-04-12]. Dostupné z: http://support.huawei.com/ehedex/hdx.do?docid=DOC1000015445&lang=en

Seznam obrázků a tabulek

Seznam obrázku

Seznam tabulek

Seznam příloh

Příloha.A: SRU a Rozšiřovací sloty

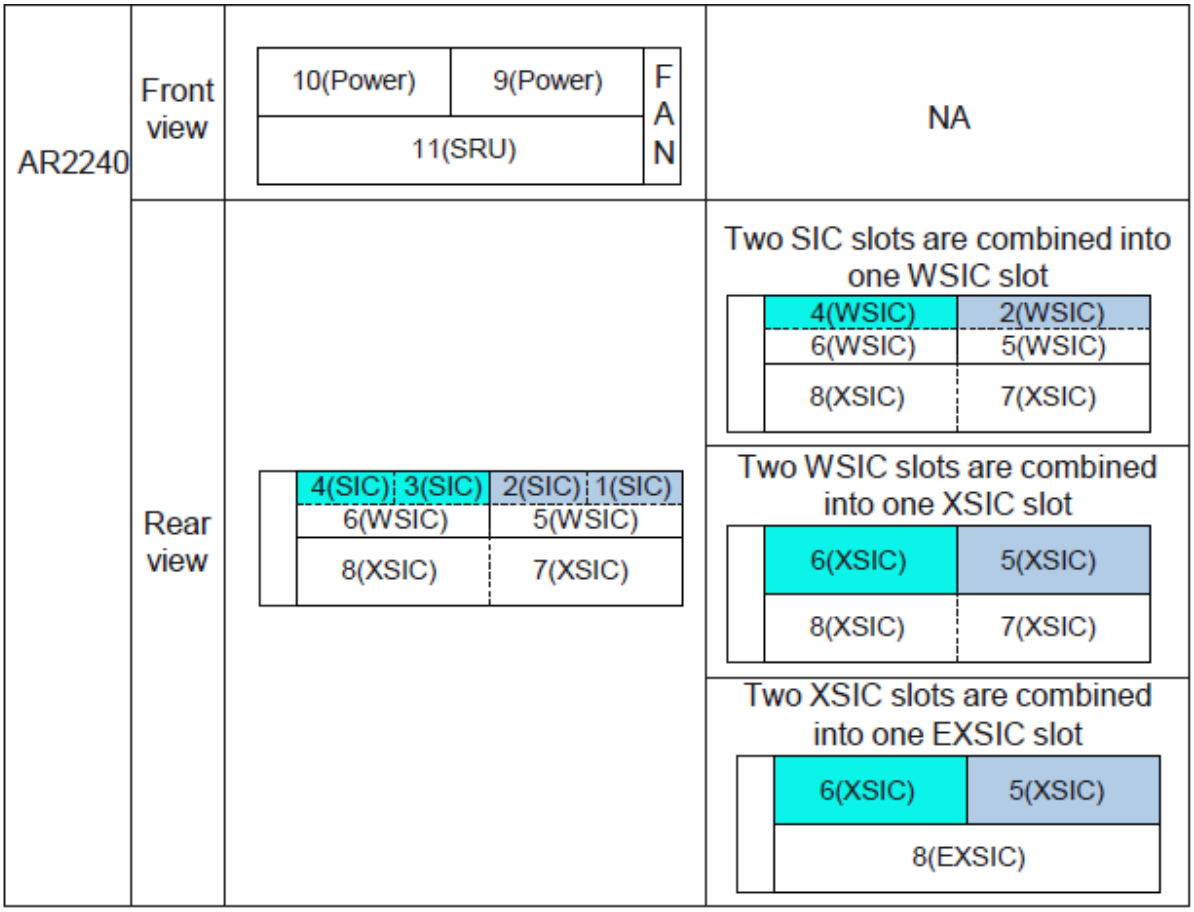
Jednotka SRU je hlavní ovládací deska na směrovačích Huawei. Jednotka SRU se dělí na tři typy SRU40, SRU60 a SRU80. Pro použití SRU jednotek velice záleží jaká verze systému je ve směrovači nahrána. Například na starší verzi systému AR V200R001C00, mohl směrovač AR2240 používat jen jednotku SRU40 a AR3260 pouze SRU80. Níže lze vidět typy SRU jednotek. [25]

Název	**Výkon**	**Forwarding capacity**
SRU40	600 MHZ CPU s 8 jádry	2 Mpps
SRU60	600 MHZ CPU s 8 jádry	2,5 Mpps
SRU80	750 MHZ CPU s 12 jádry	4 Mpps

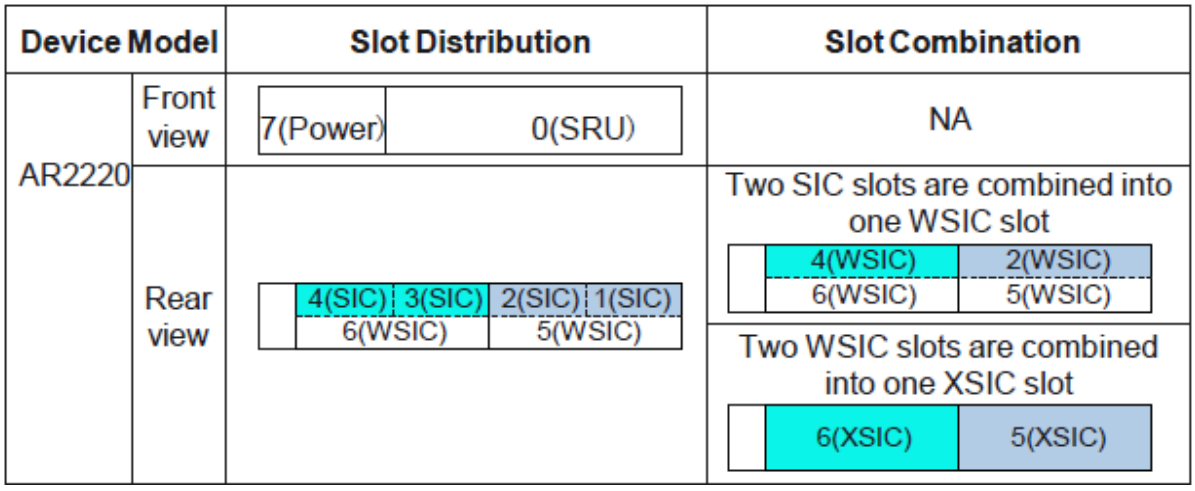
Uspořádání slotů a jejich kombinace na směrovači AR3260

<table>
<tr><th colspan="2">Device Model</th><th>Slot Distribution</th><th>Slot Combination</th></tr>
<tr><td rowspan="2">AR3260</td><td>Front view</td><td>
<table>
<tr><td>12(Power)</td><td>11(Power)</td><td rowspan="3">FAN</td></tr>
<tr><td>14(MFS)</td><td>13(MFS)</td></tr>
<tr><td colspan="2">15(SRU)</td></tr>
</table>
</td><td>Insert the SRU into slot 15.</td></tr>
<tr><td>Rear view</td><td>
<table>
<tr><td>4(SIC)</td><td>3(SIC)</td><td>2(SIC)</td><td>1(SIC)</td></tr>
<tr><td colspan="2">6(WSIC)</td><td colspan="2">5(WSIC)</td></tr>
<tr><td colspan="2">8(XSIC)</td><td colspan="2">7(XSIC)</td></tr>
<tr><td colspan="2">10(XSIC)</td><td colspan="2">9(XSIC)</td></tr>
</table>
</td><td>
Two SIC slots are combined into one WSIC slot
<table>
<tr><td>4(WSIC)</td><td>2(WSIC)</td></tr>
<tr><td>6(WSIC)</td><td>5(WSIC)</td></tr>
<tr><td>8(XSIC)</td><td>7(XSIC)</td></tr>
<tr><td>10(XSIC)</td><td>9(XSIC)</td></tr>
</table>
Two WSIC slots are combined into one XSIC slot
<table>
<tr><td>6(XSIC)</td><td>5(XSIC)</td></tr>
<tr><td>8(XSIC)</td><td>7(XSIC)</td></tr>
<tr><td>10(XSIC)</td><td>9(XSIC)</td></tr>
</table>
Two XSIC slots are combined into one EXSIC slot
<table>
<tr><td>6(XSIC)</td><td>5(XSIC)</td></tr>
<tr><td colspan="2">8(EXSIC)</td></tr>
<tr><td colspan="2">10(EXSIC)</td></tr>
</table>
</td></tr>
</table>

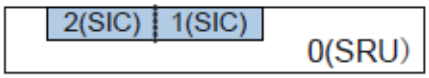
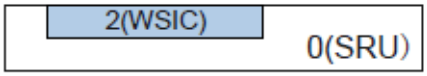
Uspořádání slotů a jejich kombinace na směrovači AR2220.



Uspořádání slotů a jejich kombinace na směrovači AR2240.



Uspořádání slotů a jejich kombinace na směrovačích řady AR1200.

Device Model		Slot Distribution	Slot Combination
AR1200	Front view	NA	NA
	Rear view		Two SIC slots are combined into one WSIC slot 

Příloha.B: Tabulky parametrů směrovačů

Tabulky parametrů pro směrovače Huawei.

	AR1220	**AR1220V AR1220W AR1220VW**	**AR2220**	**AR2240**	**AR3260**
Forwarding capacity	350 Kpps	350 Kpps	1 Mpps	2 Mpps (standard)	2 Mpps (standard)
WAN speed With services	25 Mbps	25 Mbps	75 Mbps	150 Mbps	1000 Mbps
Switching capcaity	8 Gbps	8Gbps	32 Gbps	32 Gbps	160 Gbps
WAN porty	2*GE	2*GE	3*GE	3*GE	3*GE
LAN porty	8*FE	8*FE	-	-	-
SIC sloty	2	2	4	4	4
WSIC sloty	-	-	2	2	2
XSIC sloty	-	-	-	2	4
PoE	-	4*FE	-	-	-
Wifi	-	802.11 b/g/n	-	-	-
USB 2.0	2	2	2	2	2
Mini-USB	1	1	1	1	1
Paměť	512 MB	512 MB	2 GB	2 GB	2 GB
Paměť Flash	256 MB	256 MB	16 MB	16 MB	16MB

Pokračování parametrů pro směrovače Huawei.

MicroSD	-	-	Max. 4 GB	Max. 4 GB	Max. 4 GB
Napájení	100 - 240 VAC, 50-60 Hz				
Max. výkon napájení	54 W	54 W	150 W	350 W	350 W
Rozměry (mm)	390x220x44,5		442x420x44,5	442x470x88,1	442x470x130,5
Hmotnost	2,9 Kg	2,9 Kg	4,95 Kg	8,85 Kg	11 Kg
Provozní rozsah teplot	0°C – 40°C	0°C – 40°C	0°C – 40°C	0°C – 40°C	0°C – 40°C
Doporučená relativní vlhkost	5-90%	5-90%	5-90%	5-90%	5-90%

Software	
Voice	RTP, SIP, SIP AG, IP PBX/TDM PBX, FXO/FXS, VoIP/conference call
3G	CDMA 2000 EV-DO Rev A, WCDMA, TD-SCDMA, individual 3G uplink/backup link
LAN	IEEE 802.1, IEEE 802.3, VLAN management, MAC address management, MSTP
WAN interfaces	Ethernet, CE1/CT1, E1/T1, ADSL2+, G.SHDSL, Sync/Async Serial, ISDN, CPOS, EPON/GPON
IPv4 unicast routing	Routing policy, static route, RIP, OSPF, IS-IS, BGP
IPv6 unicast routing	Routing policy, static route, RIPng, OSPFv3, IS-ISv6, BGP4+
Multicast	IGMP version1/2/3, IGMP-Snooping version1/2/3, PIM SM, PIM DM, MSDP
MPLS	LDP, MPLS L3 VPN, static LSP, dynamic LSP
VPN	IPSec VPN, GRE VPN, DSVPN
QoS	MPLS QoS, priority mapping, traffic policing (CAR), traffic shaping, congestion avoidance (based on IP precedence/DSCP WRED), congestion management (LAN interface: SP/WRR/SP+WRR; WAN interface: PQ/CBWFQ)
Security	ACL, firewall, 802.1x authentication, MAC address authentication, Web authentication, AAA authentication, RADIUS authentication, ARP security, ICMP attack defense, IP Source Guard, DHCP snooping
Management and maintenance	Upgrade management, device management, Web network management system, GTL, SNMP, RMON, Auto-Config, NetConf
WLAN (only AR1200)	AP management, WLAN QoS, WLAN security (WEP/WPA/WPA2), WLAN radio management (802.11b/g/n), WLAN user management

Tabulka parametrů pro směrovač Cisco 2801.

Cisco 2801	
Rozšiřitelné sloty	2 HWIC/WIC/VIC/VWIC, 1 WIC/VIC/VWIC, 1VIC/VWIC
DSP sloty	2
PoE podpora	Ano, 120W
USB 1.1	1
Konzolový port	1
WAN porty	2*FE
WAN podpora	Optional ADSL and G.SHDSL HWICs, DOCSIS 2.0 HWICs, and 3G HWIC
10/100 Ethernet Switch Ports	Ano
Paměť (default/max)	128 MB/ 384 MB
Paměť Flash (default/max)	64 MB/128 MB
Max. výkon napájení	120 W
Napájení AC	100V - 240V
Frekvence	47Hz/63Hz
Rozměry (š x h x v)	439mm x 419mm x 45mm
Hmotnost (bez karet)	5 Kg
Provozní rozsah teplot	0°C – 40°C
Doporučená relativní vlhkost	10-85%

IPv4 Routing Protocols	RIP v1/v2, EIGRP, OSPF,BGP, PBR, and PfR
IPv6 Routing Protocols	EIGRP, RIPng, OSPFv3, IS-IS, and PBR
VPN	DM-VPN, GET VPN, V3PN, with GRE, Easy VPN, and Cisco IOS SSL VPN
Security	ACL, firewall, URL Filtering, OS Inline Prevention Systém (IPS), Network Admission Control (NAC), VRF-aware firewall, IPv6 firewall, Cisco Self Defending Network
Management and maintenance	Upgrade management, device management, deployment using USB disk, CiscoWorks Support, Cisco IOS Embedded Event Manager (EEM), Cisco AutoInstall
MPLS	Virtual Routing and Forwarding (VRF) firewall and VRF IPsec
Voice	FXO/FXS, VoIP/conference call, VoFR, Analog and Digital voice, Direct Inward Dial (DID)

Příloha.C: OSPF – ukázka konfigurace Cisco

```
R2-C(config)# router ospf 1
R2-C(config-router)# router-id 2.2.2.2
R2-C(config-router)# network 10.0.0.0 0.0.0.3 area 0
R2-C(config-router)# network 10.0.0.8 0.0.0.3 area 0
R2-C(config)# interface serial 0/1/0
R2-C(config-if)# ip addres 10.0.0.9 255.255.255.252
R2-C(config-if)# ip ospf hello-interval 10
R2-C(config-if)# ip ospf dead-interval 40
R2-C(config-if)# cost <1-65535>
```

Příloha.D: OSPF – Výpisy směrovačů

```
[R3-Huawei] display ospf peer
          OSPF Process 1 with Router ID 3.3.3.3
                  Neighbors
Area 0.0.0.0 interface 10.0.0.6(GigabitEthernet0/0/0)'s neighbors
Router ID: 1.1.1.1      Address: 10.0.0.5
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 10.0.0.5 BDR: 10.0.0.6   MTU: 0
   Dead timer due in 36 sec
   Retrans timer interval: 5
   Neighbor is up for 01:53:30
   Authentication Sequence: [ 0 ]
                  Neighbors
Area 0.0.0.0 interface 10.0.0.13(GigabitEthernet0/0/1)'s neighbors
Router ID: 4.4.4.4      Address: 10.0.0.14
State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 10.0.0.14  BDR: 10.0.0.13   MTU: 1500
   Dead timer due in 34 sec
   Retrans timer interval: 4
   Neighbor is up for 01:53:37
   Authentication Sequence: [ 0 ]
```

```
R2-Cisco#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.0.0 0.0.0.3 area 0
    10.0.0.8 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    4.4.4.4              110      01:28:52
    1.1.1.1              110      01:22:18
  Distance: (default is 110)
```

Příloha.E: IPSec – ukázka konfigurace Cisco

```
R2-C(config)# crypto isakmp policy 1
R2-C(config-isakmp)# encryption aes 128
R2-C(config-isakmp)# hash sha
R2-C(config-isakmp)# authentication pre-share
R2-C(config-isakmp)# group 2
R2-C(config-isakmp)# lifetime 86400
R2-C(config)# crypto isakmp key test address 172.16.1.1
R2-C(config)#access-list 101 permit ip 20.20.20.0 0.0.0.255
            ->10.10.10.0 0.0.0.255
R2-C(config)# crypto ipsec transform-set myset esp-aes esp-sha
R2-C(config)# crypto map mymap 10 ipsec-isakmp
R2-C(config-crypto-map)# set peer 172.16.1.1
R2-C(config-crypto-map)# set transform-set myset
R2-C(config-crypto-map)# match address 101
R2-C(config)# interface FastEthernet0/0
R2-C(config- if)# crypto map mymap
```

Příloha.F: IPSec – výpisy směrovačů

```
[R1-Huawei] display ike peer name peer1 verbose
   Peer name                : peer1
   Exchange mode            : main on phase 1
   Pre-shared-key           : test
   Proposal                 : 1
   Local ID type            : IP
   DPD                      : Disable
   DPD mode                 : Periodic
   DPD idle time            : 30
   DPD retransmit interval  : 15
   DPD retry limit          : 3
   Peer Ip address          : 172.16.1.2
   VPN name                 :
   Local IP address         :
   Remote name              :
   Nat-traversal            : Disable
   Configured IKE version   : Version one

[R1-Huawei] display ipsec policy
IPsec policy group: "map1"
Using interface: {GigabitEthernet0/0/0}
    Sequence number: 10
    Security data flow: 3000
    Peer name:  peer1
    Perfect forward secrecy: None
    Proposal name:  proposal1
    IPsec SA local duration(time based): 3600 seconds
    IPsec SA local duration(traffic based): 1843200 kilobytes
    SA trigger mode: Automatic
    SA remaining key duration (bytes/sec): 1887436800/3537
    Max received sequence-number: 0
    UDP encapsulation used for nat traversal: N
```

```
[R1-Huawei] display ipsec proposal
 Number of Proposals: 1
  IPsec proposal name: proposal1
   Encapsulation mode: Tunnel
   Transform         : esp-new
   ESP protocol      : Authentication SHA1-HMAC-96
                       Encryption     AES-128

[R1-Huawei] display ipsec sa
Interface: GigabitEthernet0/0/0
    path MTU: 1500
==============================
  IPsec policy name: "map1"
  Sequence number  : 10
  Mode             : ISAKMP
    Connection id: 9
    Encapsulation mode: tunnel
    Tunnel local : 172.16.1.1
    Tunnel remote: 172.16.1.2
    [Outbound ESP SAs]
      SPI: 2148617108 (0x80114b94)
      Proposal: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887436800/3537
      Max sent sequence-number: 0
      UDP encapsulation used for nat traversal: N
    [Inbound ESP SAs]
      SPI: 1691711124 (0x64d57694)
      Proposal: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887436800/3537
      Max received sequence-number: 0
      UDP encapsulation used for nat traversal: N
```

```
R2-Cisco# show crypto session
Crypto session current status
Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500
      IKE SA: local 172.16.1.2/500 remote 172.16.1.1/500 Active
      IPSEC FLOW: permit ip 20.20.20.0/255.255.255.0
     10.10.10.0/255.255.255.0
            Active SAs: 2, origin: crypto map

R2-Cisco# show crypto engine connections act
Crypto Engine Connections
      ID    Type        Algorithm  Encrypt    Decrypt    IP-Address
    1001    IKE         SHA+AES          0          0     172.16.1.2
    2001    IPSec       AES+SHA          0          9     172.16.1.2
    2002    IPSec       AES+SHA         10          0     172.16.1.2

R2-Cisco# show crypto isakmp policy
Global IKE policy
Protection suite of priority 1
      Encryption algorithm:       AES (128 bit keys)
      Hash algorithm:             Secure Hash Standard
      Authentication method:      Pre-Shared Key
      Diffie-Helman group:        #2 (1024 bit)
      Lifetime:                   86400 second, no volume limit

R2-Cisco# show crypto key
Keyring          Hostname/Address                Preshared Key
Default          172.16.1.1                      test
```

Příloha.G: MPLS – ukázka konfigurace Cisco

```
R2-C>enable
R2-C#configure terminal
R2-C(config)#ip cef
R2-C(config)#mpls label protocol ldp
R2-C(config)# interface FastEthernet0/0
R2-C(config- if)# mpls ip
R2-C(config)# interface FastEthernet0/1
R2-C(config- if)# mpls ip
```

Příloha.H: MPLS – výpisy směrovačů

```
[R1-Huawei] display mpls ldp peer
LDP Peer Information Public network
A '*' before a peer means the peer is being deleted.
-------------------------------------------------------------------
PeerID          TransportAddress         DiscoverySource
-------------------------------------------------------------------
10.1.3.1:0      10.1.3.1                 GigabitEthernet0/0/2
10.1.4.1:0      10.1.4.1                 GigabitEthernet0/0/0
-------------------------------------------------------------------
TOTAL: 2 Peer(s) Found.
```

```
[R1-Huawei] display mpls route-state
Codes: B(BGP),I(IGP),L(Public Label BGP), O(Original BGP), U(Unknow)
-------------------------------------------------------------------
Dest/Mask        Next-Hop   Out-Interface    State   LSP   VRF  Type
10.1.4.0/30      10.1.1.1   GE0/0/0          READY   1     0    I
10.1.5.0/30      10.1.1.1   GE0/0/0          READY   1     0    I
192.168.2.0/24   10.1.1.1   GE0/0/0          READY   1     0    I
192.168.2.0/24   10.1.2.1   GE0/0/2          READY   1     0    I
```

```
 [R1-Huawei] display mpls ldp lsp
------------------------------------------------------------------
DestAddress/Mask  In/OutLabel  UpstreamPeer NextHop     OutInterface
*10.1.1.0/30      Liberal/3                 DS/10.1.4.1
*10.1.2.0/30      Liberal/19                DS/10.1.4.1
*10.1.3.0/30      Liberal/20                DS/10.1.4.1
10.1.4.0/30       1029/3       10.1.4.1     10.1.1.1    GE0/0/0
10.1.4.0/30       1029/3       10.1.3.1     10.1.1.1    GE0/0/0
10.1.5.0/30       1033/17      10.1.3.1     10.1.1.1    GE0/0/0
10.1.5.0/30       1033/17      10.1.4.1     10.1.1.1    GE0/0/0
*192.168.1.0/24   Liberal/16                DS/10.1.4.1
192.168.2.0/24    1034/18      10.1.3.1     10.1.1.1    GE0/0/0
                  1034/1031    10.1.3.1     10.1.2.1    GE0/0/2
192.168.2.0/24    1034/18      10.1.4.1     10.1.1.1    GE0/0/0
                  1034/1031    10.1.4.1     10.1.2.1    GE0/0/2
------------------------------------------------------------------
 TOTAL: 5 Normal LSP(s) Found.
 TOTAL: 1 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a NextHop means the LSP is FRR LSP

[R1-Huawei]display mpls ldp interface
LDP Interface Information in Public Network
Codes:LAM(Label Advertisement Mode), IFName(Interface name)
A `*` before an interface means the entity is being deleted.
------------------------------------------------------------------
IFName      Status     LAM     TransportAddress     HelloSent/Rcv
GE0/0/0     Active     DU      192.168.1.1          1287/1466
GE0/0/1     Active     DU      192.168.1.1          1395/0
GE0/0/2     Active     DU      192.168.1.1          644/629
```

```
[R1-Huawei]display isis route
              Route information for ISIS(l)
             ISIS(l) Level-1 Forwarding Table
IPV4 Destination IntCost  ExtCost  ExitInterface  NextHop    Flags
192.168.1.0/24   10       NULL     GE0/0/1        Direct     D/-/L/-
192.168.2.0/24   40       NULL     GE0/0/0        10.1.1.1   A/-/-/-
                                   GE0/0/2        10.1.2.1
10.1.1.0/30      10       NULL     GE0/0/0        Direct     D/-/L/-
10.1.2.0/30      10       NULL     GE0/0/2        Direct     D/-/L/-
10.1.3.0/30      20       NULL     GE0/0/2        10.1.2.1   A/-/-/-
10.1.4.0/30      20       NULL     GE0/0/0        10.1.1.1   A/-/-/-
10.1.5.0/30      30       NULL     GE0/0/0        10.1.1.1   A/-/-/-
                                   GE0/0/2        10.1.2.1
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP
Shortcut, U-Up/Down Bit Set


R2-Cisco#show mpls ldp neighbor
  Peer LDP Ident: 192.168.1.1:0; Local LDP Ident 10.1.4.1:0
     TCP connection: 192.168.1.1.55203 – 10.1.4.1.646
     State: Oper; Msgs sent/rcvd: 536/474; Downstream
     Up time: 01:54:48
     LDP discovery sources:
      FastEthernet0/0, Src IP addr: 10.1.1.2
     Address bound to peer LDP Ident:
     10.1.1.2   192.168.1.1     10.1.2.2
  Peer LDP Ident: 10.1.5.2:0; Local LDP Ident 10.1.4.1:0
     TCP connection:10.1.5.2.56268 – 10.1.4.1.646
     State: Oper; Msgs sent/rcvd: 222/191; Downstream
     Up time: 00:46:23
     LDP discovery sources:
      FastEthernet0/1, Src IP addr: 10.1.4.2
     Address bound to peer LDP Ident:
     10.1.4.2   10.1.5.2   10.1.3.2
```

```
R2-Cisco#show mpls ldp bindings
lib entry: 10.1.1.0/30, rev 2
           local binding: label: imp-null
           remote binding: lsr: 10.1.5.2:0, label: 1038
lib entry: 10.1.2.0/30, rev 12
           local binding: label: 19
lib entry: 10.1.3.0/30, rev 14
           local binding: label: 20
lib entry: 10.1.4.0/30, rev 6
           local binding: label: imp-null
           remote binding: lsr:192.168.1.1:0, label: 1039
lib entry: 10.1.5.0/30, rev 8
           local binding: label: 17
           remote binding: lsr:192.168.1.1:0, label: 1033
lib entry:192.168.1.0/24, rev 4
           local binding: label: 16
           remote binding: lsr:192.168.1.1:0, label: 1039
lib entry:192.168.2.0/24, rev 10
           local binding: label: 18
           remote binding: lsr:192.168.1.1:0, label: 1034
           remote binding: lsr:10.1.5.2:0, label: 1040

R2-Cisco#show mpls forwarding-table
Local  Outgoing     Prefix          Bytes Label Outgoing    Next Hop
Label  Label or VC  or Tunnel Id    Switched    interface
16     No label     192.168.1.0/24  53478       Fa0/0       10.1.1.2
17     No label     10.1.5.0/30     0           Fa0/1       10.1.4.2
18     1040         192.168.2.0/24  0           Fa0/1       10.1.4.2
19     No label     10.1.2.0/30     0           Fa0/0       10.1.1.2
20     No label     10.1.3.0/30     0           Fa0/1       10.1.4.2
```

```
R2-Cisco# show ip route
     10.0.0.0/30 is subnetted, 5 subnets
i L1    10.1.3.0 [115/20] via 10.1.4.2, FastEthernet0/1
i L1    10.1.2.0 [115/20] via 10.1.1.2, FastEthernet0/0
c       10.1.1.0 is directly connected, FastEthernet0/0
i L1    10.1.5.0 [115/20] via 10.1.4.2, FastEthernet0/1
c       10.1.4.0 is directly connected, FastEthernet0/1
i L1 192.168.1.0/24 [115/20] via 10.1.1.2, FastEthernet0/0
i L1 192.168.2.0/24 [115/30] via 10.1.4.2, FastEthernet0/1
```

Příloha.I: IPv6 – konfigurace Cisco

```
R2-C>enable
R2-C#configure terminal
R2-C(config)#ipv6 unicast-routing
R2-C(config)# interface FastEthernet0/0
R2-C(config- if)# ipv6 address 5:1::2/64
R2-C(config)# interface FastEthernet0/1
R2-C(config- if)# ipv6 address 6:1::2/64
R2-C(config)# exit
R2-C(config)# router bgp 65008
R2-C(config-router)# bgp router-id 2.2.2.2
R2-C(config-router)# no bgp default ipv4-unicast
R2-C(config-router)# neighbor 5:1::1 remote-as 65008
R2-C(config-router)# neighbor 6:1::1 remote-as 65008
R2-C(config-router)#address-family ipv6
R2-C(config-router-af)#neighbor 5:1::1 activate
R2-C(config-router-af)#neighbor 6:1::1 activate
R2-C(config-router-af)#network 5:1::/64
R2-C(config-router-af)#network 6:1::/64
```

```
[R5-Huawei]display bgp ipv6 routing-table
 BGP Local router ID is 5.5.5.5
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 8
 *>i Network  : 5:1::                                PrefixLen : 64
     NextHop  : 9:1::1                               LocPrf    : 100
     MED      : 0                                    PrefVal   : 0
     Label    :
     Path/Ogn : 65008 i
 *>i Network  : 6:1::                                PrefixLen : 64
     NextHop  : 9:1::1                               LocPrf    : 100
     MED      : 0                                    PrefVal   : 0
     Label    :
     Path/Ogn : 65008 i
 *>i Network  : 7:1::                                PrefixLen : 64
     NextHop  : 9:1::1                               LocPrf    : 100
     MED      : 0                                    PrefVal   : 0
     Label    :
     Path/Ogn : 65008 i
 *>i Network  : 8:1::                                PrefixLen : 64
     NextHop  : 9:1::1                               LocPrf    : 100
     MED      : 0                                    PrefVal   : 0
     Label    :
     Path/Ogn : 65008 i
 *>i Network  : 9:1::                                PrefixLen : 64
     NextHop  : 10:1::1                              LocPrf    : 100
     MED      : 0                                    PrefVal   : 0
     Label    :
     Path/Ogn : i
```

```
*>   Network  : 10:1::                                  PrefixLen : 64
     NextHop  : ::                                      LocPrf    :
     MED      : 0                                       PrefVal   : 0
     Label    :
     Path/Ogn : i
   i
     NextHop  : 10:1::1                                 LocPrf    : 100
     MED      : 0                                       PrefVal   : 0
     Label    :
     Path/Ogn : i
*>   Network  : 11:1::                                  PrefixLen : 64
     NextHop  : ::                                      LocPrf    :
     MED      : 0                                       PrefVal   : 0
     Label    :
     Path/Ogn : i
```

```
[R5-Huawei] display bgp ipv6 peer
BGP local router ID : 5.5.5.5
Local AS number : 65009
Total number of peers : 1                 Peers in established state : 1
Peer      V   AS      MsgRcvd  MsgSent  OutQ   Up/Down        State PrefRcv
10:1::1   4   65009        95       96     0  01:28:09  Established       6
```

```
[R5-Huawei] display bgp ipv6 network
BGP Local router ID is 5.5.5.5
Local AS Number is 65009(PublicV6)
Network     Prefix      Route-policy
10:1::      64
11:1::      64
```

```
R2-Cisco# show ipv6 route bgp
     10.0.0.0/30 is subnetted, 4 subnets
B    7:1::/64 [200/0] via 5:1::1
B    8:1::/64 [200/0] via 5:1::1
B    9:1::/64 [200/0] via 6:1::1
B    10:1::/64 [200/0] via 9:1::2
B    11:1::/64 [200/0] via 9:1::2

R2-Cisco# show ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 65008
BGP table version is 18, main routing table version 18
7 network entries using 1092 bytes of memory
10 path entries using 760 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 b of memory
BGP using 2648 total bytes of memory
BGP activity 9/2 prefixes, 14/4 paths, scan interval 60sec

Neighbor V AS   MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
5.1::1   4 65008    121     115     18   0    0 01:52:46      3
6.1::1   4 65008    108     104     18   0    0 01:39:58      5
```